PROCEEDINGS

7th International Conference on Information Law and Ethics

ICIL 2016

Broadening the Horizons of Information Law and Ethics. A Time for Inclusion

February 22-23, 2016
Pretoria
South Africa

Editors
Bottis M., Alexandropoulou E.

ΕΚΔΟΣΕΙΣ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ
ΜΑΚΕΔΟΝΙΑΣ

ISBN: 978-618-5196-25-7

The University of Macedonia Press
156 Egnatia st,
546 36 Thessaloniki, Greece
T +30 2310 891.743
F +30 2310 891.731
E uompress@uom.gr
W www.uom.gr/uompress/

Text processing: **Katerina Yannoukakou**

Lay out: **Maria Kefala**

Production editing: **University of Macedonia Press**

PREFACE

The rapid development of technologies, especially on the online environment, give rise to a wide legal discussion concerning invasion of privacy, infringement of intellectual rights, e-criminality and related scientific subjects, connected with relevant ethical issues. From this point of view, Conferences on Information Law and Ethics are not only significant but also essential, giving the opportunity to exchange knowledgeable ideas on the above subjects and evaluating the relevant scientific field.

The International Conference on Information Law (ICIL) is an international event organized by the Department of Archive and Library Science of the Ionian University, as the main organizer and it started in 2008 as an activity of the Postgraduate Program of the above Department, in Corfu, Greece. Since 2008, seven ICIL conferences took place, coorganised with other Academic Institutions, such as the Department of Applied Informatics of the University of Macedonia (Thessaloniki, Greece), the Law School of the Aristotle University (Thessaloniki, Greece) and other national and international entities.

The latest ICIL, 7th International Conference on Information Law and Ethics of 2016 (ICIL 2016) "*Broadening the Horizons of Information Law and Ethics. A Time for Inclusion*" took place on 22-23 February 2016 at the University of Pretoria (South Africa). It was co-organized by the Department of Archive and Library Science of the Ionian University and the Research Team IHRC (www.ihrc.gr), the African Centre of Excellence on Information Ethics, the Centre for Human Rights of the University of Pretoria, the Department of Applied Informatics of the University of Macedonia (Greece) and the I.T.Law Research Group (www.itlaw.uomgr), as well as the International Society for Ethics and Information Technology (INSEIT).

The thematic area covered in ICIL 2016 was wide. It included several legal and ethical aspects concerning information and its treatment in the Information Society. Apart from speakers' important presentations, including and interesting points of vews supported by young scholars, it is worth mentionning the opportunity for academics and scholars coming from diferrent continents and cultures to know each other and exchange scientific opinions.

ICIL 2016 was sponsored (morally) by the Institute for Legal Informat-

ics (IRI), the Capurro-Fiek Foundation, the NEXA Center for Internet and Society, the Journal of Intellectual Property Forum (IPSANZ), the Seattle Journal for Social Justice the International Center for Information Ethics and the Editions "Nomiki Bibliothiki" (Athens, Greece). We express our gratitude to them. Special mention and thanks are due to the Postgraduate Program in Applied Infromatics (Department of Applied Informatics, University of Macedonia) and the Special Account for Research Grants of the University of Macedonia, for sponsoring the proceedings in hand.

We also need to thank from our hearts the Honorary Chair, prof. Rafael Capurro, the General and Local Chair Prof. Theo Bothma, the Organizing Committee Chairs Nikos Koutras and Coetzee Bester, the members of Program Committee, all the speakers and chairs, as well as the members of the I.T. Law Research Group of the University of Macedonia (www.itlaw.uom.gr) Katerina Yiannoukakou and Maria Nikita for their help and support in the Conference. Special thanks are owed to Roubini Oikonomidou, MSc., for her invaluable help with the organization of this conference and the construction and update of the conference' s site. Special also thanks to Nikos Koutras, PhD (cand.), who as always contributed greatly to the conference' s success and to Katerina Yiannoukakou, PhD(cand), for her precious help in the work for this volume. And last, but not least, we need to thank our editor, the Editions of the University of Macedonia and especially Mrs. Ioanna Dandelia and Mrs. Maria Kefala for their persistent collaboration resulted in the present volume. Thank you all.

Thessaloniki, May 2017

Associate Professor Maria Bottis
Connference's General Chair/Young Scholars Forum Chair

Professor Eugenia Alexandropoulou-Egyptiadou
Conference's Paper Chair

KEYNOTES

In Search of Ariadne's Thread in Digital Labyrinths

by Rafael Capurro[1]

"Times, they are 'a changin"
Bob Dylan

1. Introduction

In 1994 a group of scholars and scientists started an initiative called "Foundations of Information Science" (FIS). The first conference was held in Madrid, followed by Vienna (1996), Paris (2005), Beijing (2010), Moscow (2013) and Vienna (2015). Focused on the concept of information, the group was well aware that different disciplines interpret this concept within their fields and theories giving rise to controversies when it comes to an interdisciplinary approach. Having participated at the Vienna conference in 1996 and, almost twenty years later, at the Vienna conference in 2015, I have also followed the discussions of the FIS group in the mailing list coordinated by the Spanish biologist Pedro Marijuán and have experienced firsthand the growing relevance of an interdisciplinary reflection on the concept of information. Information Science has several roots. One of them is its emergence in the late sixties in the context of librarianship in connection with the application of computer technology to the organization of knowledge as what was called *information retrieval*. With the rise of the Internet the concept of information addressed larger societal issues beyond the specific area of scientific communication. Although other disciplines have been using the concept of information since the 19th century, it became relevant in the engineering and telecommunication sciences, particularly since Claude Shannon's "A Mathematical Theory of Commu-

1 Professor Emeritus, Hochschule der Medien, Stuttgart, Germany. International Center for Information Ethics (ICIE), Karlsruhe, Germany.

nication" was published in 1948 (Shannon, 1948).

It is not my aim to give an overview of this complex history and its present situation (Capurro, 2009). I would like rather to discuss some of the issues dealt with in the panels and sessions in which I was involved during the Vienna conference dealing particularly with social responsibility, Critical Theory, Robotics, Global Brain, and Philosophy of Information and to summarize what I learned regarding the challenges in the field of information ethics. Secondly, I will relay the results of an email exchange that took place following the conference between a number of colleagues and myself in which we explored our perceptions of the issues at hand and the stakes involved and whether or not we were able to trace to any length the myth Ariadne's thread in digital labyrinths. I will clarify how even though digital labyrinths and threads are a part of today's societies they are often confused or even identified with society and with our being-in-the-world itself. To underline my argument, and to show how such confusion can result in mortal consequences, I will conclude by examining the case of the Chinese poet and migrant worker Xu Lizhi who committed suicide after working for Foxconn for just three years.

2. The ISIS Summit 2015

The ISIS Summit "The Information Society at the Crossroads. Response and Responsibility of the Sciences of Information" was organized by the now former president of the International Society for Information Studies (ISIS), Wolfgang Hofkirchner, at the Vienna University of Technology in June 3-7, 2015 (ISIS Summit 2015). It was the host of the 6th International Conference on the Foundations of Information Science (FIS 2015) as well as the 2nd International Conference on Philosophy of Information (ICPI 2015) and the 5th ICTs and Society Conference. The Summit hosted also several sections organized by the International Society for Biosemiotic Studies (ISBS), the International Association for Computing and Philosophy (IACAP) and the International Symmetry Association (ISA). The participants of the Summit, some 350 persons, came from 36 countries from all continents but there were only two participants from Africa, namely the philosopher John Collier from the University of Kwa-Zulu-Natal (Durban, South Africa) and, *cum grano salis*, a researcher at the African Centre of Excellence for Information Ethics (ACEIE) at the University of Pretoria,

namely myself. The participants could choose between nine tracks, namely: history of information, emancipation or disempowerment of man, empowering patients, information in the exact sciences and symmetry, informational warfare, multi-level semiosis, music, information and symmetry, searching to create a humanized civilization, and the global brain.

At the opening session there was a panel on 'Responsible Science? Meaningful Technology?' of which I had the honour to be a member together with Armin Grunwald, professor of Philosophy of Technology at the Karlsruhe Institute of Technology and Head of the Institute of Technology Assessment and System Analysis (ITAS), Gordana Dodig-Crnkovic, professor of Computer Science at the Chalrmers Institute of Technology, Sweden and now new president of ISIS, Shahram Dustdar, professor of Computer Science at the Vienna University of Technology, and the moderator Chris Frauenberger, senior researcher, Institute for Design and Assessment of Technology at the Vienna University of Technology. Armin Grunwald made an introductory speech in which he stressed the limits of consequentialism and the need for a hermeneutic assessment when dealing with ethical issues of technology. This was a remarkable speech in this context where there was a lot of discussion on social and ethical aspects of information technology based, for instance, on semiotics, system theory and critical theory but none on hermeneutics. According to Armin Grunwald, ethical and legal discussions about the consequences of technologies are embedded, mostly implicitly, in narratives that need to be made explicit in order to understand the historical context in which decisions choosing among different alternatives or scenarios are taken. I quote:

> *While the consequentialist idiom deals with assessing statements about possible futures in terms of their plausibility in order to evaluate their consequences, the hermeneutics of discourse on technological futures focuses on the meaning of these debates for contemporary attitudes towards new technologies. The 'hermeneutic turn' to view the lively and controversial debates about new fields of science or technology not as anticipatory, prophetic or quasi-prognostic talks of the future, but as expressions of our present day. The subject of investigation is not what is being said with more or less justification about coming decades, but what is revealed about us by the fact that these debates are happening today (Grunwald, 2015).*

I have been dealing with hermeneutics and information technology and Information Science since the seventies (Capurro, 1978, 1986, 2010) but I have the impression that until recently it has been a dialogue of the deaf – with famous exceptions such as Hubert Dreyfus, Terry Winograd and Fernando Flores. Philosophical hermeneutics remains mostly ignorant of the issues raised by information technology and information technology does not understand what hermeneutics is about. Armin Grunwald opened the door for an interdisciplinary debate. This debate should include, also from a hermeneutic perspective, Systems Theory, Semiotics and Critical Theory. One of the major advocates of Systems Theory and the Sciences of Information is Wolfgang Hofkirchner, professor at the Institute of Design and Assessment of Technology at the Vienna University of Technology. Semiotics was represented by, for instance, Loet Leydesdorff, professor in the Dynamics of Scientific Communication and Technological Innovation at the University of Amsterdam, with his paper "Mutual Redundancies and Triple Contingencies among Perspectives", as well as by Søren Brier with contributions on "Cybersemiotics". Christian Fuchs, Director of the Communication and Media Research Institute, University of Westminster, UK and editor of the open access journal *tripleC: Communication, Capitalism & Critique*, talked about "Critical Theory of the Internet: The importance of Raymond Williams, Dallas Smythe and Herbert Marcuse."

On the second day I participated in a forum asking the question, "Are robots better than humans? Ethics, limitations and promises of Artificial Intelligence." The objectives of this forum, co-organized and sponsored by the Catholic University Community Vienna and the Capurro-Fiek Foundation, were to analyze ethical questions arising from the spread of robots in everyday life. I quote from the announcement:

> *Do we need to grant highly developed robots rights? Do we need to equip them with ethical norms as science fiction writers have proposed? Is it acceptable to use such machines to harm humans? Are hybrid systems, i.e., humans connected to computer systems acceptable? What is the proprium humanum that distinguishes us from highly skilled robots? Highly developed computer systems and robots are important to humans and can make the world a better place.*

After short speeches by Tom Ziemke, Professor of Cognitive Science, Inter-

action Lab, School of Informatics, University of Skövde, Sweden on "The body of knowledge: Why robots aren't taking over the world – and why we are giving it to them anyway", Peter Purgathofer, Institute for Design and Assessment of Technology, Vienna University of Technology on "Hard-to-see problems in social robots" and myself on "Agents, patients and robots. About Roboethics" (Capurro, 2012) there was a debate at which Martin Rhonheimer, priest of the Catholic prelature Opus Dei and currently teaching at the Pontifical University of the Holy Cross in Rome, as well as Søren Brier, Department of International Business Communication, Copenhagen Business School, Denmark participated. The moderator was Marco Ragni, Center for Cognitive Science, Institute of Computer Science and Social Research, University of Freiburg, Germany. What struck me in this debate was the polarization between, on the one hand, a critical discourse warning about the impact of robots on society and, on the other hand, a neo-liberal position advocated paradoxically by Martin Rhonheimer who argued that in a free-market economy, consumers should decide for themselves what they want without any legal regulation. During the discussion, I argued that in democratic societies, the free decision of the consumers regarding the use of a technology takes place in an ethical and political context leading to the creation of a legal framework that should not be confused with a paternalistic view of the state in its relation to civil society. Freedom within rules means the possibility of changing rules on the basis of a critical dialogue, not only in the parliament but also through media and in academia. Without sound academic research, there is a slippery slope tendency towards polemics and lack of analysis about good and bad reasons for informed decisions. This is true not only with regard to technical but also to ethical, legal and societal issues. The field of robotics is expanding quickly into all kinds of human activities. A hermeneutic analysis about different narratives underlying the concepts of robot can help to better understand *as what* robots are being understood in different societies. Making explicit the norms and values embedded in such narratives lays the foundation for an ethical debate about the development and use of *online* robots beyond mere consequentialist reflections (Capurro, 2015).

The invention and breath-taking widespread use of the Internet gave rise from the very beginning to different kinds of cyber utopias such as John Perry Barlow's "A Declaration of the Independence of Cyberspace"

in 1996 (Barlow, 1996). Twenty years later the Internet is a global reality no less than a source for new utopias. Some of them were discussed at the Vienna conference under the label "Global Brain". I would like to mention just two interventions, one by Francis Heylighen, research professor at the Vrije Universiteit Brussel, well known for the "Principia Cybernetica Project" developed together with Cliff Joslyn and Valentin Turchin since 1989/90. His presentation "The Global Brain, a self-organizing, distributed intelligence emerging from the web" was a summary of this project based on the combination of Cybernetics and Systems Theory. Similar ideas were presented by Dirk Helbing, professor of Sociology at the ETH Zürich on "Creating a planetary nervous system as a citizen web." Without going into these cyber visions of humanity, they can evidently turn and *de facto* have already turned into dystopian realities such as global surveillance and control, cyber espionage and cyber warfare, to mention just a few. Although these dystopian aspects were considered by Heylighen and discussed in other presentations, I had the impression, at least hearing these two presentations, of a kind of cyber idealism. In the case of Heylighen, his vision is related to theological predecessors such as Pierre Teilhard de Chardin's (1981-1955) "noosphère" as well as to the visions of a universal documentation system, the "Mundaneum Palais mondial," developed by Paul Otlet (1868-1944) and Henri La Fontaine (1854-1943), and to the older visions of the encyclopaedists of the Enlightenment. Today's global brain looks like Google. I asked both speakers: 'Why do you think so much about a global brain and say nothing about a global stomach?' It was a provocative question that remained unanswered.

I also had the opportunity of meeting a young Canadian anthropologist, Cadell Last, who looks for a "pathway" to the "Global brain" based "in an understanding of evolutionary anthropological evidence of our emergence as a species and cybernetic theory" (Last, 2015).

One of the most significant features of the Vienna conference was, from my perspective, the number of Chinese participants and the quality of their presentations. I had the privilege to participate at the 2nd International Conference on Philosophy of Information (ICPI) organized by Wu Kun, professor at the Department of Philosophy of Xi'an Jiaotong University and Director of ICPI, and Joseph E. Brenner Corresponding Member, International Center for Transdisciplinary Research, Paris, Associate Director

of ICPI and ISIS Vice-President for Inter- and Transdisciplinarity. The 1st ICPI was held in Xi'an in 2013, initiated by the International Center for Philosophy of Information at the Xi'an Jiaotong University with more than 100 participants. The following remarks about the ICPI conference within the ISIS conference are focused on some of the presentations by the Chinese colleagues (ICPI, 2015). Wu Kun has been doing research on Philosophy of Information since the eighties advocating an "informational turn" in science and philosophy. In his paper "The Interaction and Convergence of the Philosophy and Science of Information" he writes:

> *Generally speaking, the Philosophy of Being, as well as the theory of the compartmentalization of the extant domain is the major paradigm of philosophy and makes up the core of philosophical metatheory. Following tradition, we can reasonably summarize ''the existential = the material + the mental" as in the traditional Western ontological paradigm, except for few doctrines out of the ordinary.*
>
> *Based on the latest progress in the science of information, the contemporary philosophy of information compartmentalizes the existential domain again. It puts forward a new ontological paradigm: ''the existential = the material + the informational". In the light of it, information is constituted by two domains: the objective informational and the subjective informational (mental). Compared with the traditional ontological paradigm, this new one not only reveals a whole fresh existential domain - the objective informational world - but also stipu1ates the essence of mind as a form of an advanced state of informational activity (Wu, 2015).*

Wu Kun obviously criticises the Cartesian split between *res cogitans* and *res extensa* or the mental and the material. To advocate a philosophical paradigm based on "the existential" equated with "the material and the informational" presupposes an interpretation of the concept of being or "existence" not only with regard to "the material" and "information" but also to our own way of being *as* being-in-the-world for whom beings become manifest *as* what they are, instead of *as* a worldless and isolated subjectivity separated from objects in the so-called outside world (Capurro, 1986). A paper by Joseph Brenner supported Wu's concept of a convergence of science and philosophy under the influence of the philosophy of information.

A contribution to this ontological debate was presented by Wu Qi Tian "A new way of thinking about being and non-being" (Wu, 2015). Wang Jian compared Wu Kun's philosophy of information with Gilbert Simondon's analysis of "the mode of existence of technical objects" as well as of the notions of form and information (Wang 2015). Li Ning Guai's "On Sign and Information-A comparison of Philosophy of Technology and Philosophy of Information" dealt with Wu Kun and Albert Borgmann (Li, 2015). In my speech "Translating Information" I argued for an intercultural philosophical dialogue on the concept of information that includes not only its Latin and Greek roots but also the translations and interpretations into Arabic, Persian, and Hebrew (Capurro, 2015, 2014a). During the discussions a Chinese colleague told me that in Chinese, the sign for information has to do with breathing. This evoked for me Daoist thinking. I remarked that the concept of information might be a way of translating Dao in the 21st century. With this remark I was also thinking about what I once learnt from Carl Friedrich von Weiszäcker about the concept of information as being a way of translating, i.e., interpreting today the Greek concepts of *eidos*, *idea* and *morphe*. This remark gave rise to my research on the etymology and the history of ideas of this concept in the seventies (Capurro, 1978).

3. An email exchange after the conference

After the conference an email exchange took place among a number of colleagues and myself in which we evaluated some of the philosophical and societal issues at hand and the stakes involved and whether or not we were able to trace to any length the myth of Ariadne's thread in digital labyrinths. For those who may not be familiar with this myth, I can first say briefly that it is a myth about a guide to freedom, which is not a myth at all but something we all have a need for. As for the concept of labyrinth itself, its design and initiatory function, I note that it is part of many cultural heritages throughout the world (Kern, 1999). I use the concept of labyrinth in order to address issues of knowledge and power that might allow us — but who constitutes 'us' and who are we in the digital age? — to become agents of change and not just digital 'sub-jects', i.e. objects of private monopolies and state powers and unable to develop new shapes of freedom (Capurro, 2014). In order to do this, we must be aware that our being-in-the-world

with others is not identical with the reification of ourselves on the Internet. I call this the ethical difference.

Following the path of thought about considering the Dao *as* information, I sent an e-mail to Xueshan Yan from the Department of Information Management, Peking University, — who could not take part of the ISIS conference but who is a member of FIS — asking him about the Chinese sign for information and its relation with breathing and information. He answered me as follows:

> *The expression of Information in Chinese is* 信息（*pronunciation: xin xi). 信 in ancient Chinese has the meaning of "say something by mouth", "letter"; in modern Chinese it means message (informal or small information); only 息 has the meaning of breathing both in ancient and modern Chinese. If separated 信 or 息 do not have any relationship with Dao. Only when they are combined together the meaning of Dao can emerge (Xueshan Yan, e-mail from September 8, 2015).*

Joseph Brenner found this issue being closely related to his research on "Logic in Reality" (Brenner 2008). We started a conversation about the book of the French philosopher and sinologist François Jullien: "La grande image n' a pas de forme" (Jullien, 2005). The title is a quote from Chapter 41 of the Tao Te Ching: "The great form has no shape" (Laozi, 2011). Jullien analyses the way or *Dao* of the indeterminate that is expressed in classical Chinese with words such as air, wind (*feng*) or atmosphere. Wind circulates or 'impregnates' what is and what is not: "The grass must bend, when the wind (*feng*) blows across it." (Confucius, 2005, xii,19). This differs from the Platonic and Aristotelian views that matter is 'in-formed' by forms. It goes, in fact, in the opposite direction to the Western *method -hodos* means 'way' in Greek- that starts with the indifferentiated, the mythical *chaos*, Aristotle's *hyle* (matter) or Plato's *chora* (receptacle or material substratum) being 'in-formed' by the *demiurge*, a kind of "artisan god" (Margel, 1995). According to Jullien, the Chinese painter starts with form (*xing* 形) and goes through a dynamism or vitality (*shi*) or through wind or air (*qi-xiang* 氣象) in such a way that what is eventually depicted is *informis* or without form. This makes possible that the forms which are at the bottom and not at the top open themselves to the indeterminate. The pictorial result is the

"great image that has no form." (Jullien, 2005/2009) Joseph Brenner sent me the following quote in the English translation from François Jullien's *La grande image*. He found that the translator uses the form breath-energy, breath-image, breath-phenomenon, breath-resonance and breath-spirit for the words in French starting with *souffle:*

> *The Chinese also conceived of atmosphere by means of another binomial linked to wind and explicitly associating the visible and invisible.[…] The energy of the undifferentiated foundation (of the world) actualizing itself and taking form, this image (phenomenon) spreads out as a 'breath-atmosphere'. Wang Wei indicates this as a principle: "When one contemplates the painting, one must look first at the breath-image; then the tonality – clear or confused, limpid or opaque; then the relation structuring (the structural relation of) the principal and secondary mountains (Jullien, 2009, Transl. Jane Marie Todd).*

This understanding of information *as* no-form is the opposite to the results of my early research on the etymology and history of ideas of the Latin term *informatio* as a translation of the heavy Greek metaphysical terms *eidos, idea, morphe* and *typos* (Capurro, 1978). I followed the track of *informatio* as documented in the "Thesaurus Linguae Latinae" (ThLL) where it is stated that *informatio* is composed of the particle 'in' meaning a reinforcing and not a negation of the forming process (*formatio*). Although the particle *in* means also 'no' — like the *alpha privativum* in Greek for instance in *a-letheia* (un-concealment, truth) — no use of this sense with regard to *informatio* is given, excepting related concepts such as *informabilis*, *informia*, *informitas*, and *informiter*. In my dissertation I mentioned this but did not follow the track further. This has been done now by Vinícios Souza de Menezes, a PhD student in Information Science at the Brazilian Research Center for Information (IBICT), and an expert in contemporary philosophy in his paper "Information, a critical-philological excursus" in which he critically analyzes my interpretation (Menezes, 2015). What remained forgotten in my analysis leads him to *informatio* as *aletheia* and to Aristotelian and Platonic metaphysics with the predominance of beings and not of being as a process of giving. This path of thinking makes possible a translation between *informatio* as no-form and the Chinese thinking of the Dao -as well as with the Japanese tradition *Musi* or 'denial of self' (Nakada and

Tamura, 2005; Capurro, 2005)- through the mediation of Western thought on the abyss of existence by some philosophers quoted by Menezes such as Wittgenstein, Heidegger and Agamben. In my paper for the first Chinese conference on Information Ethics that took place at the Renmin University in Beijing in 2010 (Capurro, 2010a), I quoted Chuang Tzu:

> *Fishing-stakes are employed to catch fish; but when the fish are got, the men forget the stakes. Snares are employed to catch hares, but when the hares are got, men forget the snares. Words are employed to convey ideas; but when the ideas are apprehended, men forget the words. Fain would I talk with such a man who has forgot[en] the words! (Chuang Tzu 26, 11)*

A main issue in my presentation at the ICPI conference in Vienna dealt with the relation between language and information as analyzed by Carl Friedrich von Weizsäcker (Weizsäcker 1973) and Martin Heidegger (Heidegger 1959). This *hermeneutic* relation is also an *angeletic* one -from Greek *angelos* = messenger)- , dealing with the transmission and mutual exchange of messages and not only with their interpretation, Hermes being both, the messenger of the gods and their interpreter (Capurro and Holgate 2011, Capurro 1978, 263-266). Michael Eldred writes:

> *Above all, the mutual exchange (metabole) of messages, the interplay of messaging in which an attentive listening to each other on the part of the interlocutors is essential. All exchange presupposes a mutuality of some kind, no matter how defective (Even subjugation to the other is a kind of exchange.). Mutual exchange is a kind of (at least) double or (complex multiple) movement resulting from the intertwining of the exercise of the powers of the exchangers (Michael Eldred, e-mail from September 9, 2015).*

Following the discussions on social and ethical issues during the Vienna conference, a group of colleagues — among them Rainer E. Zimmermann, professor of Philosophy at the University of Applied Sciences in Munich, and José María Díaz Nafría, engineer and philosopher, professor at the University of León (Spain) and creator of BITrum, a glossary of concepts, metaphors and theories dealing with information (BITrum, 2015)-, came to the idea of creating a research group called SE 104. The acronym corresponded

to the room where a session of the Vienna Summit on ethical issues of the information society took place that had the particularity of being difficult for the participants to find! This was also a general issue for most participants searching for their session rooms in the labyrinthine building of the Technical University of Vienna. The title of this group was given with a good sense of humour but addressed also a serious issue, namely whether the theories proposed and discussed during the Summit were Ariadne's thread(s) in the digital labyrinths and/or labyrinth(s) in themselves. I suggest using also the plural form, since there are several possibilities for shaping freedom when facing digital labyrinths and threads and also because, as José María Díaz Nafría suggested in one of his mails, digital labyrinths seem to have no center with one Minotaur, one Ariadne, and one Theseus. According to the myth, Crete's King Minos was in opposition to the kings of Athens for whom his palace was a labyrinth, i.e., a centre of power and domination. The labyrinth was built by Daedalus, a famous craftsman, for King Minos to imprison the Minotaur. The Minotaur, half-man, half-bull is a symbol of evil since his only role in existence was to eat maidens sacrificed by Minos to his gods. Minos' daughter, Ariadne, was willing to help Theseus, the son of King Aegeus of Athens, in whom she fell in love, in his task to kill the Minotaur by giving him a sword and a ball of thread to find his way out of the labyrinth. Today, we are inside digital labyrinths guided by threads that look like Ariadne's but often make us unable to be aware of the labyrinth *as* a labyrinth, i.e. as a place of negative power and domination. They are threads of business, not of love.

In his "History of Philosophy" Hegel writes that to know that "a human being is free" makes an "incredible difference" ("ein ungeheurer Unterschied") in human history although such knowledge does not mean its realization (Hegel, 1971, 40). It is not a question of looking for an outside to the digital labyrinth(s) in the sense of avoiding the historical challenges of the digital age. It is, instead, a question of how far we are able, again, to see the labyrinth *as* a labyrinth, i.e., to unveil knowledge and power in digital age as done, for instance, by Edward Snowden. I agree with Peter Fleissner, professor emeritus of Design and Assessment of New Technologies at the Vienna University of Technology, that any restriction by social, political and economic structures hindering the emancipatory development of people is an essential indicator for the transformation of the present information so-

cieties. Freedom is not a property of a worldless and isolated subjectivity, but a relation between human beings in a shared world that is concerned with their mutual respect and fairness also in their relation to the natural world to which we belong. Both relations, to ourselves and to the world, are today mediated by digital technologies. They give rise to the belief that *to be* means *to be digital* and, particularly, that I am a human being only as far as I am in the digital world reifying or 'in-forming' my self *as* digital data and believing that I *am* eventually a digital being. I call this belief *digital metaphysics* that I distinguish from *digital ontology*, in which the digital *understanding* of being is acknowledged as *a* possible today predominating way of understanding ourselves and the world. The difference between 'is' and 'as' is not only an ontological but an ethical one (Capurro, 2012a). The ethical difference between *who* and *what* we are, or between our selves and our data, is one of Ariadne's threads (Capurro, Eldred, Nagel, 2013).

The task of *translating information* in the sense I proposed at the Vienna Summit can be understood as one of Ariadne's threads of emancipation from the knowledge and power structures of the digital labyrinth. Looking for a language of "mutuality" (Peter Fleissner), i.e., of mutual estimation and care for each other, in the digital age means looking for mediations that depend on our capacity to translate our concepts and values into other languages and *vice versa*, to be open to the messages coming from the other(s) particularly when they look *uncanny*, i.e., unusual or unfamiliar from a *normal* perspective, an issue that led Thomas Kuhn to his theory on the structure of scientific revolutions (Kuhn, 1962; Capurro and Holgate, 2011). This is not only a theoretical but also a practical task about different kinds of exercises of resistance and resilience at the macro- and micro-levels in order to transform ourselves and our societies into more free and fair ones in the digital age (Capurro, 1995).

4. Conclusion: a poet's voice

In September 30, 2014, Xu Lizhi (aged 24), a Chinese poet and migrant worker, from a peasant family, committed suicide after three years' working for Foxconn, a Taiwanese multinational, manufacturing products such as iPad, iPhone -"Designed by Apple in California Assembled in China"- Kindle and PlayStation with plants in Shenzhen in mainland China. The Ger-

man sinologist and journalist Kai Strittmatter published in June 2015 a long article "The Leap" ("Der Sprung") in the German newspaper *Süddeutsche Zeitung* telling the story of Xu Lizhi who tried to survive the strange coupling of communism and capitalism in the 'perfect city' of Shenzhen. Strittmatter writes:

> *The workers come from China, the boss from Taiwan, the profits go to Apple and we all touch gently the tools. The Communist Party finds itself in a peculiar role: it came to power fighting for the proletarians, but now, suddenly, it is on the exploiters' side (Strittmatter, 2015, my translation).*

Xu Lizhi, Strittmatter tells us, was one of 300 million workers who left the countryside searching for work in the city. Shenzhen was a small fishing village near Hong Kong of about 30.000 inhabitants thirty years ago. Today some ten million people live there. Xu Lizhi is a poet who hated serial production, the city, and the factory. When he was 19 years old, he discovered literature reading Yu Hua's (born 1960) novel "To Live." A year later he leaves the small town and goes to Shenzhen. February 17, 2011 is his first working day, a night shift, at Foxconn, with one day off a week. He is fascinated by the public library and by a bookshop called "Bookbar", open day and night. He meets a tour guide there. She is 38 and was born in the city. They talk about the growing gap between rich and poor in China. It is forbidden to speak on the conveyor belt. "It is like at the time of Charlie Chaplin's 'Modern Times'" writes an editor of a Shenzhen literary journal. Xu Lizhi's generation dreams of dignity, freedom and meaning. Xu Lizhi flees. He reads (Li Bai, Du Fu, Shakespeare, Baudelaire, Faulkner, Tagore, Rilke, Adonis) and writes:

"I swallowed an iron moon
They call it a screw
I swallowed the factory's sewage
The unemployment documents
Youth, bending over the machines
Dies before its time
I swallowed the drudgery [...]

I swallowed the rusty life
Now I can't swallow any more
Everything I swallowed
Gushes from my throat
Pours over the land of my ancestors
Into a shameful poem."
Xu Lizhi
(transl. from German by RC)

He meets like-minded persons on the Internet. The poet Yan Lian says that socialism talks about the people "but until now it is the dumb people." Now the poets come and give the proletarians a voice. Xu Lizhi tries to find a way out of a slave's work in the factory's library. No chance. At the beginning of 2014 he quits Foxconn. His microblog has no entries. In September 26 he comes back to the "place of execution" (Xu Lizhi, quote from Schrittmatter, 2015: "Hinrichtungsstätte") and signs a new contract with Foxconn. Four days later, at 2pm, he jumps from the 17th floor of the AAA Bureau and Shopping Mall with a broad view of the Chinese dream and of a Kindergarten with the letters "Self Confidence." His last poem "My last moments" begins:

"I want to see the sea once more."
The last lines are:
"It was fine with me when I arrived
It is fine with me when I go."

5. References

1. Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Online: https://projects.eff.org/~barlow/Declaration-Final.html.
2. BITri (2010). Glossary. Online: http://glossarium.bitrum.unileon.es/glossary.
3. Brenner, J. E. (2008). Logic in Reality. New York: Springer.
4. Capurro, R. (2015). Living with Online Robots. Online: http://www.

capurro.de/onlinerobots.html.

5. Capurro, R. (2015a). Translating Information. Online: http://sciforum.net/conference/isis-summit-vienna-2015/paper/2972.
6. Capurro, R. (2014). Shapes of Freedom in the Digital Age. In H. S. Keseroğlu, G. Demir, E, Bitri, and A. Güneş (eds.): 1st International Symposium on Philosophy of Library and Information Science. Ethics: Theory and Practice. Istanbul: hiperlink 2015, 1-13. Online: http://www.capurro.de/kastamonu.html.
7. Capurro, R. (2014a). Apud Arabes. Notes on Greek, Latin, Arabic, and Persian Roots of the Concept of Information. Online: http://www.capurro.de/iran.html.
8. Capurro, R. (2012). Toward a Comparative Theory of Agents. In: *AI & Society*, 27 (4), 479-488. Online: http://www.capurro.de/agents.html.
9. Capurro, R. (2012a). Beyond Humanisms. In Toru Nishigaki and Tadashi Takenouchi (eds.): Information Ethics. The Future of the Humanities, Nagoya City: V2 Solution Publisher 2012, 26-74. Online: http://www.capurro.de/humanism.html.
10. Capurro, R. (2010). Digital hermeneutics: An outline. In: AI & Society 35 (1), 35-42. Online: http://www.capurro.de/digitalhermeneutics.html.
11. Capurro, R. (2010a). The Dao of the Information Society in China and the Task of Intercultural Information Ethics. Online: http://www.capurro.de/china_infoethics2010.html.
12. Capurro, R. (2009). Past, present and future of the concept of information. In *tripleC*, 7 (2), 215-141. Online: http://www.capurro.de/infoconcept.pdf.
13. Capurro, R. (2005). Privacy. An Intercultural Perspective. In *Ethics and Information Technology,* 7, 1, 37-47. Online: http://www.capurro.de/privacy.html.
14. Capurro, R. (1995). Leben im Informationszeitalter. Berlin: Akademie Verlag. Online: http://www.capurro.de/leben.html.
15. Capurro, R. (1986). Hermeneutik der Fachinformation. Munich/Freiburg: Alber. Online: http://www.capurro.de/hermeneu.html.
16. Capurro, Rafael (1985). Epistemology and Information Science. Report

TRITA-LIB-6023 Royal Institute of Technology Library, Stockholm, Sweden. Online: http://www.capurro.de/trita.htm.

17. Capurro, R. (1978). Information. Ein Beitrag zur etymologischen und ideengeschichtlichen Begründung des Informationsbegriffs. München: Saur. Online: http://www.capurro.de/info.html.
18. Capurro, R., and Holgate, J. (2011). Messsages and Messengers. Angeletics as an Approach to the Phenomenology of Communication. Munich: Fink.
19. Capurro, R., Eldred, M., and Nagel, D. (2013). Digital Whoness: Identity, Privacy and Freedom in the Cyberworld. Frankfurt: Ontos (de Gruyter).See also: Johannes Buchmann (ed.): Internet Privacy. Berlin: Acatech (2012). Online: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Projektberichte/acatech_STUDIE_Internet_Privacy_WEB.pdf
20. Chuang, Tzu (2001-2009). The Complete Chuang Tzu Based on James Legge's Translation. Online: http://oaks.nvg.org/zhuangzi25-.html#26.
21. Confucius (2005). Analects (Transl. James Legge). Online: http://www.gutenberg.org/cache/epub/3330/pg3330-images.html.
22. FIS (Foundations of Information Science). Online: http://fis.sciforum.net/about-fis/.
23. Grunwald, A. (2015). Responsible Research and Innovation - Limits of consequentialism and the need for hermeneutic assessment. Online: http://summit.is4is.org/programme/schedule/day-one-wednesday-3-june-2015.
24. Hegel, G. W. F. (1971). Vorlesungen über die Geschichte der Philosophie. Frankfurt: Suhrkamp, vol. 18.
25. Heidegger, M. (1959). Der Weg zur Sprache. In: ibid.: Unterwegs zur Sprache. Pfullingen: Neske, 83-155.
26. ICPI (2015). International Conference on Philosophy of Information. Online: http://sciforum.net/conference/isis-summit-vienna-2015/stream-icpi.
27. ISIS Summit (2015). Online: http://summit.is4is.org/programme.
28. ISIS Summit (2015). All contributions. Online: http://sciforum.net/conference/isis-summit-vienna-2015/page/allcontributions.

29. Jullien, F. (2005/2009): La grande image n' a pas de forme ou du non-objet par la peinture. In ibid.: La philosophie inquiétée par la pensée chinoise. Paris: Seuil, 263-573 (Engl. transl. Jane Marie Todd: The Great Image Has No Form, or On the Nonobject Through Painting, Univ. of Chicago Press 2009).
30. Kern, H. (1999). Labyrinthe. Erscheinungsformen und Deutungen. 5000 Jahre Gegenwart eines Urbilds. München: Prestel 4th ed.
31. Kuhn, T. (1962). The Structure of Scientific Revolutions. The University of Chicago Press.
32. Last, C. (2015). The Advanced Apes. Evolutionary Science for a Changing World. Online: http://theadvancedapes.com/pathway-to-the-global-brain-a-lecture/.
33. Laozi (2011). Daode Jing (transl. Charles Muller). Online: http://www.acmuller.net/con-dao/daodejing.html#div-42.
34. Li, N. G. (2015). On Sign and Information-A Comparison of Philosophy of Technology and Philosophy of Information. Online: http://sciforum.net/conference/isis-summit-vienna-2015/paper/2961.
35. Margel, S. (1995). Le tombeau du dieu artisan, précédé de "Avances" par Jacques Derrida. Paris: Minuit.
36. Menezes, V. S. de (2015). Informação, um excurso crítico-filológico. In: *Perspectivas em Ciência da Informação*, 20 (1), 3-18. Online: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2074.
37. Nakada, M., and Tamura, T. (2005). Japanese conceptions of privacy: An intercultural perspective. In *Ethics and Information Technology* 7, 1, 27-36.
38. Shannon, C. E. (1948). A Mathematical Theory of Communication. In *The Bell System Technical Journal*, Vol. 27, pp. 379–423, 623–656. Online: http://worrydream.com/refs/Shannon%20-%20A%20Mathematical%20Theory%20of%20Communication.pdf.
39. Strittmatter, K. (2015). Der Sprung. In: *Süddeutsche Zeitung*, Nr. 139, June 20-21, 11-13.
40. Wang, J. (2015). The Constructive Approach of Informational Ontology and the Transform of Philosophical Notion - the Comparison to the Philosophy of Information of Simondon and Wu Kun. Online: http://

sciforum.net/conference/isis-summit-vienna-2015/paper/2960.

41. Weizsäcker, C. F. von (1974). Sprache als Information. In: ibid.: Die Einheit der Natur. Munich: dtv, 39-60.
42. Wu, K. (2015). The Interaction and Convergence of the Philosophy and Science of Information. Online: http://sciforum.net/conference/isis-summit-vienna-2015/paper/2943.
43. Wu, Q. T. (2015). A New Thinking Way About the Being and Non-Being. Online: http://sciforum.net/conference/isis-summit-vienna-2015/paper/2880.
44. Yan, X. S. (2011). Information Science: Its Past, Present and Future. In: *Information*, 2, 510-527. Online: http://www.mdpi.com/2078-2489/2/3/510.

Acknowledgements

Thanks to Joseph E. Brenner (Switzerland), Jared Bielby (Canada) and Michael Eldred (Cologne) for their criticisms and assistance in polishing this text.

Rich and Varied Ethical Standards: Intellectual Freedom as a Universal Value in a World of Many Cultures

by Paul Sturges[2]

1. Introduction

Intellectual freedom is a concept of central importance to a progressive society: at all levels of educational provision; in the media; in research and debate; in politics and business; and in information institutions such as libraries. We therefore need to feel confident in our understanding of its meaning and the precise nature of its significance. It is easy for those who work in a climate of intellectual freedom to assume that respect for intellectual freedom is the global norm. It is particularly easy if you live in a country whose citizens have enjoyed intellectual freedom for centuries; if you have access to global and local networks that can provide virtually any information that might be desired; if you work with like-minded colleagues from a number of other countries; and if you know you have valued the protection offered by Article 19 on Freedom of Expression of the United Nations' Universal Declaration of Human Rights (1948).

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."*

At the very least, under such circumstances, you might tend to assume that intellectual freedom is the norm to which humankind aspires. You might assume this even when you know that many societies, states, legal systems, religions and other belief systems seek to suppress all or some of its aspects. Therefore, it is helpful every once in a while to be reminded that this not necessarily the case.

A gently probing question from an audience member after a lecture in Edinburgh on aspects of intellectual freedom delivered in 2015 was a re-

2 Professor Extraordinary, University of Pretoria, South Africa.

minder of this doubt that intellectual freedom is either universally, or even widely, accepted by the totality of humanity. When faced with this question, it was necessary to concede that intellectual freedom, although identified in Article 19 as having universal application is, however, far from universally accepted. The following is a sketch of a speculative and very tentative exploration of responses to the question. The intention is to provide a more solid and reliable basis for the concept 'intellectual freedom' than mere reassertion of Article 19. Before this is possible we need to say something about the use of the term intellectual freedom. The term includes freedom of opinion (although someone's opinions need never be revealed and in that case cannot be challenged); freedom of expression (which is the term used in Article 19 somewhat confusingly to include freedom of opinion) and freedom of access to information (which is an essential underpinning for intellectual freedom). What is said in this essay applies very much to each of these three, so the inclusive term intellectual freedom is preferred to the more commonly used freedom of expression.

We will begin by looking at the challenges that are offered to intellectual freedom when we treat it as a cultural expression. Secondly, we will offer some remarks on what is suggested if we adopt a social psychology perspective. In both of these cases we will draw inferences from the seemingly unrelated, but in fact very revealing, example of human responses to homicide. Both cultural and social psychology approaches cast substantial doubt on the universality of intellectual freedom, but two further approaches can be offered as counter-balance. For the first of these we will look at relevant aspects of the philosophy of Information and Library Science (LIS) before finally turning to the science relating to brain development and childhood learning.

2. Intellectual freedom as cultural phenomenon

In May 2014 an organisation called the Organisation of Islamic Cooperation (OIC) offered a stark challenge to an Article 19-based version of intellectual freedom. A Saudi Arabian court had found Raif Badawi guilty of breaching laws that control use of information technology, and of insulting Saudi religious figures. He had set up a website called Saudi Arabian Liberals, as a forum for political and social debate. More specifically he

was accused of ridiculing Saudi Arabia's religious police, the Commission on the Promotion of Virtue and Prevention of Vice. His sentence included imprisonment, a very large fine, a ban on his media use and travel, and 1,000 lashes. Amnesty International and other NGOs condemned the verdict, and they were joined by a small number of principled politicians willing to risk offending the rulers of one of the world's most wealthy and influential countries. Margot Wallstrom, the Swedish Foreign Minister, was prominent among these. However, it is the response to Wallstrom made by the Organisation of Islamic Cooperation (OIC) which offers the most interesting scope for discussion. In defending the verdict, it refers to the world's 'rich and varied ethical standards' (OIC, 2015). At first glance this seems like a ridiculous use of the language of the tourist brochure to defend a cruel and excessive punishment for what was a simple exercise of freedom of expression. However, if were merely to brush off the claim that ethical standards vary and that (by implication) we should celebrate this, that would be an inadequate response. Recent work on intercultural information ethics, notably by Brey (2007), Capurro (2008) and Bielby (2015) generally makes the important point that ethical systems, including those relating to information, are cultural phenomena that need to be understood in context.

For the sake of argument we could easily accept the OIC's use of the words 'varied ethical standards'. We can take the use of the word 'standards' in the sense of 'norms' rather than implying levels of quality in the way it is often used. So in this sense the OIC has the right to cite the existence of varied ethical standards when it talks of an intellectual freedom matter such as the Badawi case. Indeed it is not hard to identify deep-rooted cultural differences that potentially clash with what the Universal Declaration claims are the true values. It is communal values that inform and inspire ethical thinking in the societies of very large parts of the world: pretty certainly in most parts. What matters in such societies is family and the wisdom and love of the father (and mother); the guidance of local chiefs, politicians, elders and cultural figures; the teachings of priests and other religious leaders, and the tenets of their faiths; and the directives of elected politicians, non-elected leaders and monarchs. In such societies people help and support each other, but they also control each other and suppress deviant ideas and impulses before they can even clash with orthodoxy. For the unques-

tioning such societies are comfortable and supportive. For those driven to ask questions, they are unbearably stifling and have to be challenged or quit in favour of some freer intellectual climate.

The expression of culture in behaviour and ideas varies greatly across the range of human concerns. We will use as an example of the interplay between society, the individual and ethical thinking, an example so strikingly different that it might seem totally irrelevant. This extreme example is cultural attitudes towards homicide; the killing of other human beings. On the surface, homicide seems to be rejected across the world. Most religions, cultures and judicial systems quite simply deal with killing as an unlawful action, except under rigidly prescribed instances of self defence or non-culpable accident. The duel and the blood feud have been effectively driven out of society in most European countries for some centuries now, although the feud is said to linger on in Albania, Georgia and one or two other places. It is important, however, to stress that cultural prohibition of killing by individuals is not completely universally established. For instance, the Masai of Kenya and Tanzania find it hard to accommodate to the justice systems of the countries in which they live. Among their difficulties is the sense in their culture that if a man is provoked beyond endurance, for him to kill the offending person in fair fight is natural and not particularly reprehensible. More extreme than this, amongst the Afar people of Eastern Ethiopia, it has been normal for a man to express his manhood by killing others. The killing need not be provoked or in any sense 'justified'. Another man's life, even when taken in a cowardly and deceptive way, could be celebrated by a knotted string attached to the killer's belt. These are exceptions, but they remind us that there is some level of cultural propensity to kill which exists across societies and cultures.

We must also remember the irony that the judicial systems of various countries reserve to themselves the right to punish some offences, including not only murder, but rape and drug-dealing, by execution. What is more, public opinion as represented in commentary, opinion polls and referendums consistently favours capital punishment as an appropriate response to certain crimes. Iran, China and some states of the USA can be mentioned in the context of judicial killing. In all of these it is undoubtedly the case that judicial killing is to some extent culturally sanctioned whilst killing by an individual is not. Countries also maintain armies, have poli-

cies on national defence, and wage war with depressing frequency. Thus, we have the situation in which societies and the judicial systems they create have chosen to outlaw killing by individuals whilst all of them reserve this same right to themselves and employ large numbers of people trained as soldiers and equipped to kill. With this example in mind, we can go beyond simply accepting that cultures vary. We can agree with the OIC that the ethical reasoning and standards that cultures carry with them varies too. Furthermore, if we probe under the surface of ethical thinking, we can identify propelling forces that are neither entirely common to all humanity, nor the product of an untrammelled individuality.

3. Social psychology and intellectual freedom

Ironically, a beautifully clear and warm expression of the universalist viewpoint on intellectual freedom came from an atheist on the day in 1697 when he was about to be executed for the crime of blasphemy. Thomas Aikenhead, a student in Edinburgh, said:

> *It is a principle innate and co-natural to every man to have an insatiable inclination to the truth, and to seek for it as for hid treasure. (Graham, 2008, p. 118).*

Those who condemned him in court and put the rope around his neck were effectively seeking to refute this claim in the most extreme imaginable way only hours after he had made it. Aikenhead's claim depends on a vision of human beings as individuals obliged to take full responsibility for their own ideas and actions. To a large proportion of the world's population this would probably seem a ridiculous claim that could only be made by a rash fool. Their incredulity would be based, at least in part, on their cultural background. But there are more elaborately layered dimensions of social psychology that are likely to be relevant. There are a host of feelings, thoughts, beliefs, intentions and goals that are constructed in relation to human beings' relations with others, at a variety of levels from family and small groups to society as a whole. Such psychological factors influence behaviour and attitudes and undoubtedly condition the acceptance or rejection of an importance stance like support for intellectual freedom.

Rather than addressing the manifestation of social psychology directly

in terms of intellectual freedom, we can usefully return to the example of homicide. The speculations about social psychology that emerge from the example can be argued also to suggest underlying patterns that might also relate to intellectual freedom attitudes and practices. Given that we accept that cultures have mixed attitudes towards homicide, we can ask the question as to whether this reveals some natural pattern in human psychology. It is in the military experience that we can perhaps find some clues as to whether killing is natural to humans, although largely suppressed by laws. It is clear that some soldiers can kill, but some are simply psychologically unable to do so. Indeed, a well known suggestion is that only 15 to 20% of men (and women too?) are capable of bringing themselves to deliberately kill another (Grossman, 1996). This suggestion is largely based on the much-contested findings of S. L. A. Marshall regarding soldiers in the First World War. Marshall's contention was that most men in combat avoided firing directly at the enemy. A possible restatement of this is possible without entirely dismissing Marshall's contention. This would be to say that there is a proportion of up to 20% (including a few for whom killing brings a kind of psychological fulfilment), who can kill and who seem to suffer no psychological damage from it. Individuals from the remaining 80% sometimes can kill but they might well be those who today are identified as going on to suffer post-traumatic stress (PTS). In summary, we could say that killing is natural for only a few and unnatural for the majority: that, indeed, there is a spectrum of human responses to homicide.

The variation of response and, indeed, confusion that applies to killing in its various forms might well also apply all other aspects of human propensities. Unfortunately, we have no reliable way at present of knowing what percentage of people are inherently drawn towards the various aspects of intellectual freedom we listed earlier (freedom of opinion, freedom of speech, freedom of access to information). However, survey data does tend to suggest that the patterns of human psychology vary according to a frequently recurring 80:20 distribution. For instance, we might be talking here about a similar proportion to Marshall's 15-20% who could kill, as embracing an extreme positions (that, indeed, of Aikenhead) in favour of intellectual freedom. What if, for the sake of argument, we were look less at the figure of 20% than the 80% majority which felt differently? This 80% is certainly not an undifferentiated mass: it will include shades of opinion.

We might then ask if the survey evidence (fragmentary though it might be) could also be turned to suggest a further 20% from that majority who might firmly reject intellectual freedom. This would give us a spectrum (or even a Bell Curve) of difference with 20% minorities at either end and an apathetic central 60%. The curiosity of this majority would go little beyond the narrow promptings of the need for information for daily life and work, or hobbies and leisure activities, as well as the widespread enthusiasm for gossip and trivia. A diagrammatic representation might look like this:

Spectrum of Responses to Intellectual Freedom

20%	60%	20%
Intellectual Passivity	Limited Desire for Knowledge	Free Minds
Accept Authority	Concentrate on Gossip and Trivia	Question Everything
Don't Ask Questions	Pursue Leisure Information	Explore Dangerous Ideas
Suppress Others	Acquire Work and Daily Life Information	No Limits

Is there any reported survey data which might offer a little support to the speculation embodied in this diagram? The answer is 'Not much': survey after survey in the intellectual freedom area reports 20% minorities with a strong opinion and a remaining 80%. Typical is a global survey of attitudes to online privacy (Big Brother Watch, 2013) that showed 21% of respondents not concerned and 79% revealing various levels of concern. One or two examples do, however show a distribution similar to that in the diagram above. For instance, there is a survey of opinions on Internet censorship (Depken, 2006). From a responding population of 4,247 in the USA, 25% agreed strongly with some form of restriction on publishing on the Internet, and 28% disagreed strongly. The percentages are higher than the tentative speculation we have made here, but the pattern is similar. A more recent survey of privacy and security (Madden, 2014) suggests that 18% of respondents disagree strongly with government monitoring of phone calls and Internet communication, whilst a similar proportion agree strongly. Perhaps a more intense trawl of reported surveys might reveal more, but

the honest answer is that without fuller reporting and some slightly different surveys the speculation remains unproven. What is clear is that surveys, whether they report an 80:20 distribution or something more like a Bell Curve, confirm that Article 19 is an expression of faith rather than a solidly rooted response to human propensities and cultural conditioning. This might seem a rather a pessimistic view of humanity, However, we are not obliged to accept its implications, nor do we have to accept that cultural perspectives and social psychology are the only ways of looking at intellectual freedom.

4. 'Richness in ethical standards and social psychology from an LIS perspective'

The OIC statement's use of the word rich clearly implied that we ought to accept that in some parts of the world intellectual freedom will be partially suppressed or wholly denied in religion, law and social practices. However, what if we argue that the consequences of suppressing intellectual freedom are deeply damaging to human progress? This is the beginning of a counter argument that says 'Yes, cultures and social psychology reject or ignore intellectual freedom, but we have to work *as if* humanity believed in free minds and free expression of what was in those minds'. This kind of progressive argument might not be scientific, but it does have a compelling logic in a world that depends on imaginative solutions to a host of problems in science, technology, economics and politics. Further good reasons for refusing to accept the dominance of cultures and psychological propensities emerge from the discipline of modern LIS. There are various LIS principles such as neutrality and equitability in services, or confidentiality between professional and information seeker, which are based on a progressive vision of information service. They have been developed in the crucible of professional debate and adopted by generations of librarians for good practical reasons.

Another significant professional principle is that of access to information, which relies in part on the distinction between text (or content) and format. Essentially, this suggests that library and information work is first and foremost about content, with concerns about format secondary. Thus, although most librarians devote some attention to the preservation and conservation of information materials (principally manuscript and printed

documents) and some specialist librarians have these concerns at the very centre of their professional activity, it is what manuscripts, books, audio and visual recordings, digital and online materials tell us that actually matters. From this viewpoint, no format or copy outweighs the importance of the message that is carried. This would obviously be open to the criticism of philistinism if applied to a medieval illuminated manuscript, but it carries the implication that copies of outdated popular works or school textbooks can cheerfully be pulped for recycling. This is not the place to debate this in full, but if we accept that it is in fact central to library practice, it can drive our understanding of challenges to library practice from a strong perspective of professional ethics.

A revealing example is developed by Crowley (2015, p. 207) who cites difficulties over how libraries treat copies of the Qu'ran in their collections. This is not a specifically Islamic case: something similar might apply in the case of Christian and other scriptures. Indeed, Scientologists have called for special treatment of their donations of material to libraries (Sturges and Gastinger, 2014). In Crowley's example, advice was obtained from an Islamic scholar by an American academic library to the effect that:

1. Non-Muslims should not handle the Qu'ran,
2. Physical handling of the Qu'ran should be with a cloth or glove,
3. The Qu'ran should not be placed on the floor or near feet,
4. The Qu'ran should not have other books or items placed on top of it,
5. The Qu'ran should be kept closed when not being read.

He also cites a suggestion from another source that all religious texts should be kept on a top shelf so that none was above the other. At first sight these stipulations do not look too problematic: they could be adopted without much disruption to the practices of a library. At the same time it is hard to swallow the final one of these suggestions because it depends on a horribly confused use of the word *above*. This utterly ignores the difference between *above* in a spatial sense, and *above* indicating a degree of respect. This could perhaps be ignored in the interests of harmony, but, the question remains: should librarians compromise their 'content over format' principle in the interests of peace and quiet?

The difficulty has two layers. The first concerns text. The plea for special treatment of copies of the scriptures is first based on the claim that they are 'holy' or 'sacred'; that is, true in a special way that demands distinctive

treatment over and above that granted to any other text. This would be less of a problem if there were not many rival scriptures claiming this special status to the exclusion of the others. It would also not be a problem if there were no suspicion that all scriptures were flawed in one way or another and unworthy of special treatment as a category of text. This problem could perhaps be overcome by a resolution to offer special treatment to the texts as a gesture of tolerance and social inclusiveness but that does not overcome the problem of format. Respect for a text is basically a matter of good manners; thoughtful and polite speech and behaviour. But respect for a particular copy or a whole format requires actions that are based on what librarians might regard as a fundamental confusion between text and the format which conveys it. The question arises with scriptures as to which is holy: the oral tradition from which most emerge, manuscript copies of early versions of the text, printed copies, sound and audio recordings, digital versions? Is it all of these, or just some and is one version more holy than others?

This is not a frivolous question. The case of Farkhunda exposes the issue in stark clarity (Kargar, 2015). In March 2015, in Kabul, Afghanistan, Farkhunda, a volunteer teacher and student of Islamic law was accused by a mullah of burning pages of a Qu'ran. There was no evidence to prove this ever happened and the mullah seems to have quarrelled with Farkhunda because of her criticism of his selling of religious charms. A mob gathered, beat her to death, burned her body and threw it in the river. Police allegedly stood by while this atrocity happened. Some imams and mullahs later endorsed the murder. All this would be horrible enough if it were not for the fact that Farkhunda was one of those devotees who had memorised the whole of the Qu'ran. Which raises the question as to which was more holy, the allegedly burnt book, or the living human repository of the text? The example exposes the illogicality of the demand that printed paper carrying a 'sacred' text should be afforded special status. Respect for different cultures can sure only go so far and potentially catastrophic violation of the carefully worked out principles of a modern profession like librarianship looks too far.

5. Intellectual freedom and the human brain

There is another more fundamental and universal line of reasoning that

emerges from the swiftly expanding knowledge of the human brain that is brought to us by twenty first century neuroscience. Neuroscientists use the evidence of case studies, non-intrusive experimentation and, crucially, the measurements that can be obtained from technologies that include electroencephalography, positron emission tomography (PET), functional magnetic resonance imaging (fMRI), and magnetoencephalography (MEG). These various forms of scanning allow experimenters to identify the parts of the brain that are active during many kinds of mental activity. This, in turn, offers insights into learning, problem solving and instinctual responses. For the non-scientist there is a positive outpouring of books, journalism and broadcasts that popularises neuroscience's findings. Anyone who scans the reviews of books in the quality newspaper press may well have noticed that in the last decade there has been a flow of titles introducing neuroscience to a popular audience, for example, Winston (2003), Ramachandran (2004), Rose (2006), and more recently Churchland, (2013) and Kaku, (2014). Articles in magazines and quality newspapers, many of them in the form of book reviews, are simply too numerous to mention. A valuable summary of the content of articles that have appeared in New Scientist has proved particularly useful (New Scientist: the Collection, 2015). It is necessary to admit that much of what appears in this popular literature is speculative, and some of it quite fanciful, but there are solid useful lessons there too. In particular, the growth of this popular literature makes it possible to offer a more specific rationale for the line of argument sketched out in Sturges (2006).

If we look at what popular neuroscience reports on discoveries relating to childhood learning we immediately find a great deal that applies to intellectual freedom. Evidence suggests that a flow of sensations into the child's brain that range from tastes and smells through to the visual and auditory reception of incredibly complex messages coded in language, number and other sets of symbols, does not merely inform, it develops and supports the ability to think. Babies can be observed responding to the messages from their senses as early as the moments when they first seek to attach their lips to their mother's nipple. Very quickly the baby begins to identify other sensations, recognise them when they occur, and even predict their recurrence. Soon this amounts to knowledge of their immediate surroundings and recognition for those who care for them. A process of change and growth in the brain is central to this development of understanding, but

that in turn is reliant on the reception of a flow of stimuli. Neuroscientists can measure the increase of brain activity in the areas associated with the various senses during the early months of human life. The neural equipment of the infant human has the basic capacity to cope with the information that reaches it, but more than that, the brain requires it. The baby's brain is much more plastic than the adult's and the flood of sensations is responsible for the specific form it takes. Through all of this we can see an emerging sense of self and the acquisition of language reinforcing and developing each other, to form a human being with reasoning capacity and a set of useful memories.

The significance of all of this is that it is biological and universal. Scientific opinions on what is happening in a baby's brain (conscious and unconscious) will certainly change and expand. The functions of the various organs of the brain and their neural connections are still only partially and imperfectly understood. What is, however, clear is that it is dangerous in the extreme to interfere with the processes by which the baby is exposed to stimuli and to limit the range and richness of the stimuli. The baby needs to be exposed to sounds, sights and other physical sensations, and it also needs talk, stories, songs and exposure to books. The baby exercises a kind of basic intellectual freedom which we can support and nurture by allowing it to follow its propensities but offering a banquet of sensations and communication from which it can choose. The alternative is unthinkable, because it points towards an imperfect developed brain less capable than it might be of independent and creative thought. The brain's processing speed slows down with age, but this does not hinder powerful mental activity because of the neural connections laid down in the earliest years of life and over a lifetime of learning and experience. Very recent research suggests that measurable levels of intelligence seem to be based as much as 40% on inheritance (genetic factors), but all children enter the world as active shapers of their personal environment and learning styles. This gives them the possibility to maximise their learning and compensate for the disadvantages of genetic inequality. A stronger and clearer case for intellectual freedom it is hard to imagine. By this line of reasoning intellectual freedom is indeed a human right of the most utterly fundamental kind.

The child's brain demands, and intellectual freedom allows, the processes that the brain sets in motion to function to the best effect. Maybe the circumstances of later life mean that only a part of the adult population

fully gains the advantage offered by an early exposure to information and ideas, and the freedom to meditate, speculate, and formulate concepts and new ideas. The logic of this is that educators, creators and information professionals must seek to maximise exposure to information and ideas so that the benefits are spread as widely and deeply as possible.

6. Concluding remarks

So, we concede that cultures have significant differences in their ethical approaches, and that this encompasses the information environments that they provide. Furthermore, when we explore some elementary aspects of social psychology, we concede that the adult population of the world might well be content with its position within a spectrum of responses to intellectual freedom (a spectrum including distaste for freedom and the difficulties inherent in it). However, conceding the possible truth of these propositions does not mean that it is wrong to oppose their implications from the perspective of LIS professional values. In support of this professional position is the suggestion that there remains a substantial rationale for treating intellectual freedom as a human right. This rationale is rooted in the implications of modern neuroscience. Research is beginning to support the long-established perception in progressive pedagogy that, although the adult might well settle into positions in a spectrum of responses to intellectual freedom that include indifference and hostility, the same is not true of the child. The child does not make choices as to whether it wants to learn or not: it learns with hectic speed and intensity as a condition of its being. It is the child that benefits most from intellectual freedom. Therefore we support freedom of opinion, expression and access to information first for the child and then for the adult, in the confidence that, if this does not always produce a new human being, it at least protects, nurtures and expands the most creative and effective segment of the adult population that intellectually free children can become. This is why we cling to Article 19 and why all those who facilitate intellectual freedom are essential servants of humanity.

7. References

1. Bielby, J. (2015). Comparative philosophies in intercultural information ethics. Confluence: online journal of world philosophies. 2(1). Available

at https://scholarworks.iu.edu/iupjournals/index.php/confluence/article/view/540. (Accessed 20/2/2017).

2. Big Brother Watch (2013). New research: global attitudes to privacy online. Available at https://www.bigbrotherwatch.org.uk/2013/06/new-research-global-attitudes-to-privacy-online/ (Accessed 20.2.2017).
3. Brey, P. (2007). Is information ethics culture-relative? International Journal of Technology and Human Interaction. 3(3), pp. 12-24.
4. Capurro, R. (2008). Intercultural information ethics. In: Himma, K. and Tavani, H., The Handbook of Information and Computer Ethics. New Jersey: Wiley. pp. 639-665.
5. Churchland, P. (2013). Touching a nerve: the self as brain. New York: WW Norton and Co.
6. Crowley, B. (2015). Developing information and library theory for a conflicted paradigm world. Libri, 65(3), pp. 207-216.
7. Depken, C. (2006). Who supports Internet censorship? First Monday 11(9), 4th Sept 2006. Available at Firstmonday.org/ojs/index.php/fm/article/view/1390/1308 (Accessed 20.2.2017).
8. Graham, M. (2008). The blasphemies of Thomas Aikenhead: boundaries of belief on the eve of The Enlightenment. Edinburgh: Edinburgh University Press.
9. Grossman, D. (1996). On killing: the psychological cost of learning to kill in war and society. London: Little, Brown and Co.
10. Kaku, M.(2014). The future of the mind: the scientific quest to understand, enhance and empower the mind. New York: Doubleday.
11. Kargar, Z. (2015). Farkhunda: the making of a martyr. BBC News. Available at www.bbc.co.uk/news/magazine-33810338 (Accessed 20.2.2017).
12. Madden, M. (2014). Public perceptions of privacy and security in the post-Snowden era. Pew Research Center Nov 12, 2014. Available at www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (Accessed 11.1.2016).
13. New Scientist: The Collection (2015). The Human Brain. 2(1).
14. Organisation of Islamic Cooperation (2015). OIC expresses it's

reservations. Available at: http://www.oic-oci.org/oicv2/topic/?t_ref=3915&lan=en (Accessed 20.2.2017).

15. Ramachandran, V. (2004). A brief history of human consciousness: from impostor poodles to purple numbers. New York: Pi Press.
16. Rose, S. (2006). The twenty-first century brain: explaining, mending and manipulating the mind. London: Vintage.
17. Sturges, P. (2006). 'Why intellectual freedom matters'. In: Information, Innovation, Responsibility: Information Professional in the Network society. Proceedings of the 14th BOBCATSSS Symposium, 30th Jan. – 1st Feb. 2006. Tallinn, Estonia. Tallinn: Department of Information Studies, pp. 431-439.
18. Sturges, P. and Gastinger, A. (2014). Libraries, donations and freedom of expression: The case of Scientology. Journal of Librarianship and Information Science, 46(1), pp. 32-40.
19. United Nations (1948). Universal Declaration of Human Rights. Available at http://www.unhcr.ch/udhr/lang/eng.htm (Accessed 20.2.2017).
20. Winston, R. (2003). The human mind and how to make the most of it. London: Bantam Books.

Acknowledgement

The author wishes to thank Ed Venables of the Edinburgh University Humanist Society for the questions he asked after a presentation on March 25th 2015. This essay is an attempt to find a valid response.

FREEDOM OF INFORMATION AND EXPRESSION

a. Theory

Implementation Factors and Access to Information based on Documentation Principles

by Zachou Vichelmina[1]

The historian's attempt to reconstruct the past must focus on any point of the previous times. Indeed, each element can indicate the new theories and any type of testimony can help to better accompany the event. Many researchers, for example B. Croce, harshly criticized the theoretical possibility of allocation of resources to different kinds incorporating the concept of "presumption" any type of evidence[2].

However, there is need to distinguish and analyze different types of sources to find the appropriate criteria of their conservation, classification and cataloging, so that it can be correctly used and sufficient critical appraisal. The researcher of contemporary history is exposed to a variety of sources and has to face a double problem, that of determining the archival sources relevant and accessible to his research and that of combining their use with other nature resources, whose typology and quantity is naturally richer in modern history than the more ancient history. Indeed, apart from archival sources, books, newspapers and any type of printed documentation or other cultural testimonies, the investigator of modern history can refer to audio-visual means such as pictures, radio, television, cinema, and in oral testimony, in the same medium memory. However, this multiplicity of sources makes it difficult to analyze the events which appear less homogeneous and more fragmented. The analysis can be performed backwards while viewing forward and is becoming increasingly shorter the closer the

1 Vichelmina Zachou is a historian, a PhD holder and teaches at the Ionian University.
2 B. Croce, *Teoria e storia della storiografia*, Laterza, Bari 1927, p.13.

research is to the present day[3].

In the presentation of an age, the historian must capture the political, human and social reality that crystallized on abstract and bureaucratic shapes of an official act. The historian also needs to know how to find, in the imaginative display of individual and collective events, the reflection of the political and economic structures, theories, customs and traditions, prejudices, myths and emotions. When using a source, the historian should know the creator, the typical characteristics of the environment where the source was found, the legal expediencies and the historical development on which the source is placed.

The identification and selection of the most important sources is a problem associated with the complexity of the modern state: the more we approach nowadays, so multiply the underlying decision-making capacity, where the variation of local abilities is considerable. For a modern historian, it seems problematic to take the State as a research unit, especially since the analysis of interactions appears determinative between the different states, the different geographical areas and the different cultures. It is not difficult to identify a corpus of sources not only due to the complexity of the historical, material, ideological relations, but also because of a large volume of knowledge. Today it is perhaps even more difficult to put at the core of the investigation historiographical nodes, the perspective by which we must analyze them and the theoretical foundations to address them. The State is an entity of which it is easy to present institutional elements, but it is not possible to analyze the historical events without considering that autonomy is strongly influenced by external factors, while internally a fragmentation tendency of central authority is evident. The connection of the events of a State body with the financial statements, the technological evolution of ideology, as well as the defined political balance is a historical constant from medieval times to the present day[4].

Freedom of the press and thus autonomy of information, does not of course mean objectivity of information, but by comparing different sources a problem arises regarding visual interpretation. The problem for researchers of modern history is that due to the lack of a uniform processing of the

3 F. Chabod, *Lezioni di metodo storico*, Laterza, Bari 1969, pp.58 ss.

4 G. Barraclough, *Atlante della storia 1945-1975*, Roma-Bari 1978.

principles governing the typical procedures of activity of public administration, history is expressed through the multiplicity of acts that are difficult to classify and are governed by specific rules. Sometimes specific provisions on the formal procedures of acts within it to the discretion of public administration are missing and increasing with the passage of time is the tendency of modulation from procedure. More difficult is the analysis and evaluation of the agencies' documents which lack a definite bureaucratic organization and a well-established tradition. The variety of the way of execution of the act makes the analysis and the evaluation of documents more complicated, not only for anyone who has to arrange the documents provided by a file, but also for anyone to use for research purposes. It is obvious how useful, for example, it is to recognize the typical elements that link the acts of a particular typology and allow the reconstruction of a bureaucratic system. The archivist sets the study of the documents on the historical-institutional base upon which the act was produced.

The study of documents brings up the relation between the nature of the legal instrument and the type of instrument and points out, in response to the historicity of the content of act, the typical characteristics of the document. Therefore, this study requires more legal analysis than historical. However, because the document is simultaneously a historical testimony of a legally significant act, it is a multi-faceted subject of research and analysis[5]. It is difficult to maintain a balance between the legal aspects and the historical analysis and so, there should be a harmony between them. Diplomacy is the science that studies each document separately, mainly analyzing the typology, the external and internal characteristics to define the legal nature of acts both in relation to their type and in relation to their effects. There is a rich and established tradition in the study of medieval document, while more rare are studies on documents of modern times. The current provisions of the public administration is manifested through acts that have a specified type and in some cases are determined by law. But the diplomatic analysis of documents is linked to how the document was created, to the intention expressed to the legal instrument and to the form in which this act is manifested, i.e. to the characteristics of the document

5 R. De Felice, *L' archivio moderno nella pubblica amministrazione*, ed. ANAI, Roma 1969; M. Toscano, *Storia dei trattati e politica internazionale*, Torino 1970.

by which the act is represented. Initially, we have to distinguish the legal instrument from the document: the instrument is not always written, nor has it always a prescribed model. On the other hand, not all written acts are constitutional and documentation instruments within a file.

A document is the written testimony of an event that has been prepared with the observance of certain forms, which are intended to provide faith and give probative value to them[6]. Based on this definition three basic elements are outlined that reflect the document: 1. The event to which the written testimony referred, 2. The legal nature of the act contained in the document, 3. The type of drafting that gives the document specified characteristics. It can be assumed that, if the diplomatic medieval document elaborates on these three elements, it will be possible to have power also as a diplomatic contemporary document. The written form of a modern document can be found *ad substantiam* or *ad probationem*, to give the act constitutive or probative value. The same distinction is true for the medieval document and so, many researchers[7] talk about a substantiating document - about an act that was born and perfected independently from the written form - and about a disposal document (*dispositive*) - which needs a specified written form to become a perfect document. Brunner was the first to mention this, who called *notitia* (or *breve*) the substantiating document and *charta* (or *chartula*) the disposal document. Brunner was based on the special nature of the documents and on the purpose they were serving. So Brenner distinguished substantiating documents *faits accomplis* of acts with reference to the past and documents indicative of a disposal of the author with reference to the future[8].

6 C. Paoli, *Diplomatica*, new ed. G. C. Bascapè, Sansoni, Firenze 1942 (rist. 1969), p. 18.

7 A. Pratesi, *Genesi e forme del documento medievale*, Jouvence, Roma 1979, pp. 25 ss.

8 H. Brunner, *Zur Rechtsgeschichte der römischen und germanischen Urkunde,* Berlin 1880 (rist. Aalen 1961). F. Brandileone, *Le così dette clausole al portatore nei documenti medievali italiani* (del 1903), *Origine e significato della "traditio chartae"* (del 1907), *Le così dette clausole al portatore nelle carte di alienazione degli immobili* (s.d.), *Nota preliminare sull' origine della "stantia" o "convenientia"* (del 1923), *La "stipulatio" nell'età imperiale romana e durante il medioevo* (del 1928), in Brandileone, *Scritti di storia del diritto privato italiano*, edit. by G. Ermini, II, Bologna 1931, pp. 89-146, 59-87, 213-277, 407-418, 419-528; L. Schiaparelli, *Note diplomatiche sulle carte longobarde.* III: *La formula "post traditam (chartam)"*. IV: *La formula "post traditam (chartam)" e la "traditio chartae ad proprium" del Chartularium Langobardicum* (del 1933). V: *La formula*

The question of the functions of the document relates to the reasons for its existence, the role it plays in economic and social context and the positions in the legal provision, especially in the environment of legal practice. But the terms provision, practice and documentation are concepts that necessarily refer to people who live, move and act within an environment characterized by them.

But who are the people involved in producing documents, that are behind a papyrus or a parchment or even behind a computer? During the production process of a document, the coefficients are three, *the author*, *the recipient* and *the editor*. Because such people emerge only through theoretical schemes and therefore are anonymous, which according to the case every time acquiring specific roles, we can attribute in any document two subjects or protagonists: *the sender - creator* and *the recipient*[9]. The sender - creator of a legal act [instrumentum] (Aussteller-Urheber, in German) is the person (or persons or organ) who ordered or commissioned the document and in whose name the same document acquired the title in order to become creator-author. The creator is the person who carries out, directly or indirectly, the legal or administrative instrument, which will be reflected in the document, even if they are not the author. Often the author of the instrument and the creator of the document is the same person. However, they may be different persons, for example when someone, through a document, gives approval to a particular instrument or when someone provides the "solution" to a dispute in which he is mediator. Behind every document there is always a creator, even when the document is created with the recipient's request.

In many documents the heading may be pre-printed and usually bears the indication of the authority issuing the act, even a symbolic image rep-

"sub stipulatione et sponsione interposita" (del 1934), in Schiaparelli, *Note di diplomatica (1896-1934)*, edit. by A. Pratesi, Torino 1972, pp. 248-301; H. Steinacker, *"Traditio chartae" und "traditio per chartam", ein Kontinuitätsproblem*, "Archiv für Diplomatik", 5-6 (1959-1960), pp. 1-72; G. Costamagna, *L'alto Medioevo*, in M. Amelotti - G. Costamagna, *Alle origini del notariato italiano*, Roma 1975 (Studi storici sul notariato italiano, 2).

9 F. De Lasala-P. Rabikauskas, *Il documento medievale e moderno*, Roma 2003, pp. 44-45; S. N. Asonitis, *Introduction to Latin Diplomacy,* Thessaloniki, 2011, pp. 22-23. See also M. Bottis, The Law of information, Nomiki Bibliothiki 2004.

resenting the state, the province, the municipality. There are also many documents produced by the public administration, such as records, official orders, decisions, accounting actions, and so forth, in which the header can be found typewritten or handwritten. In correspondence, the heading is mainly pre-printed and bears the indication of the institution which adopted the act, while the specific indication of the office which handled the agreement where the document originated, may be located in the header or even in the part used in the protocol classifications.

In the public administration the creator of the act may coincide with the creator of the document. There are, however, acts for which the documentation activity is entrusted to a different person and not to the original creator of the act: for example, the drafting practices, i.e. the consecutive sequence narratives of the oral statements and acts. The person who records the minutes is a "public official" who can be the holder of a public office (secretary, inspector, police officer, etc.) or a professional (for example a notary, doctor) as provided by law.

In the field of private law, it is essential to distinguish between public and private writings. A public act is the document that has been prepared in accordance with the formalities required by the notary or by a public official authorized to deliver public faith where the act is implemented. It therefore follows that in the public act, the creator of the document is different from the person who expresses the will represented in it.

In the case of the private act, the creator of the document coincides with the person who expresses the will. In this kind of acts, the signature is particularly important. Indeed, the law recognizes that the private writing has probative value unless the contrary is proven. The person who appears as the creator of a private act may renounce the signature so as the person may refuse to accept the photographic, cinematographic or other reproductions as true. The producer of these documents is required to demonstrate their compliance. The same thing happens with the photographic or photocopying copies which if failing to carry a certificate of conformity with the original by the authorized public officer, can be disclaimed.

The *recipient*, in legal terms, is the person (or persons or body) to which the document is addressed and distinguished strictly from the creator. Also called *beneficiary* (for example the buyer to a sales act or the heir to a testamentary act) who receives the document and usually preserves it to its

file as testimony. The beneficiary does not always coincide in law with the recipient of the document (for example the administration of a wedding prohibition which was sent to the general priest of a diocese has as beneficiaries the Christians who receive it). The recipient can benefit from the content of the document or be obliged to perform. His role, even when causing the issuance of the document, is passive. According to the founder of modern diplomacy, Theodor von Sickel, many princely documents, completely authentic, have been prepared and written with the care of their recipients, who then submitted them to the public authority, to deposit on them the confirmatory signs, such as a stamp, a certificate, signatures e.tc. Then, the recipient has the document so to use it as evidence whenever needed.

From a diplomatic and archival point of view the verification of the recipient' s identity in principle is an element of prime importance both to identify the file, determine the sequence and the composition of files and to the reconstruction of bureaucratic practices followed. Similar to what happens to the creator, the identification of the recipient becomes important if it is connected to the nature of the document and to whether it is an original or a copy. For the reconstruction of a series of local legal instruments all of the same nature - ministerial decrees, criminal or civil decisions, wills e.tc. - it is crucial to know the author while the recipient of each instrument is generally insignificant.

The sender/creator and the recipient are the persons connected to the document and should be represented in the document through particular types and legal considerations. In reality, the production and the design of a document is often due to the recipient requested, for example in the case of a land purchase and sale document, where the sender is the seller and the recipient is the buyer. Diplomacy often invites the author of the act: this is a fine report that may overlap the documentation that interests us. It would therefore be advantageous with clarify or to strongly indicate that it is about the author of documented instrument, i.e. so as referred to the document since even in a purchase and sale contract (which is a consensual obligation) the legal authors are two, the seller and buyer[10].

10 C. Paoli, *Diplomatica*, Sansoni, Firenze, 1942,(n. ed.): G.-C. Bascapè in *Manuali di fi-*

The author is the one who, at the creator's command or the recipient's request, writes or and validates the document. The person who writes on behalf of others mentioned in ancient documents (6th-8th c.) as *rogatarius*. It is common that the authors of the same document are more than one person, depending on the point at which each of them interferes in the steps of the document configuration. This often happens in public documents, where various officials involved, each with specific duties.

In the document, witnesses can be displayed. These can be distinguished in witnesses of act and witnesses of documentation. In the case of hegemonic acts, the presence of witnesses or bystanders, who are important representatives of the institution (for example the *procures Palatii* and the *consistorium Principis*, the nationals of the medieval empire, the cardinals of the Church), puts of important questions regarding the balance and the "constitutional" axis of reference frame every time[11].

Apart from the persons representing the document, there are those who implement it, i.e. the factors or the producers of documents. In general, we can say that a document has been prepared and produced:

- Either in the case where sender and author are the same and in this case, we are talking about manuscripts according to the ancient Greek term, autograph, holograph, i.e. all written by the hand of the creator, since in these cases the autograph signature is enough.
- Or by the scribe, *scriba*, notary, i.e. by someone who has the writing ability and the capacity of use terms and types of technical character or by a professional scribe who is registered in the list scribes by notary of Late Medieval period or end by notary of subsequent (modern) era (from the late 12th century to the present). Therefore, the author is both a freelancer and a public official, the holder of a public function such as the certification of (legal) document's authenticity.
- Or from other agents producing documents such as secretaries,

lologia e storia, serie I, vol. I, Casa editrice Le Lettere, Firenze, 1987, p.20; A. Pratesi, *Genesi e forme del documento medievale*, Roma, 1986, p. 35.

11 H. Bresslau – H. W. Klewitz, *Handbuch der Urkundenlehre für Deutschland und Italien*, I, Lipsia 1912-1932 (rist. Berlin 1958), [in ed. it.: *Manuale di Diplomatica per la Germania e l'Italia*, ed.. by A. M. Voci-Roth, Roma, 1999 (Pubblicazioni degli Archivi di Stato. Sussidi, 10), pp. 721, ss. 842 ss. 861 ss.

chancelleries, offices e.tc.

All these aspects will be analyzed under the historical period they represent. For example, the second case, from the medieval scribe-notary to the modern notary, refers to a long and multifaceted historical reality, mainly western, which directly or indirectly influenced Greece.

In the third case[12] on the production environment and dismissal of documents, the historical data support two points:

1. A document produced by a chancellery initially requires a bureaucratic, structured and multifaceted route (*iter*) of documentation for historical periods. For example, initially there could be brochures, reports (*preces*, *supplicationes*), requests, a report by referendarii, the mediation of someone or the *consulatio* of the ruler in the case of institutional decisions. In the phase of documentation, announcers (*dictatores*) could exist who understand the text (in some cases the technicians of law and politics, such as the «vir magnificus quaestor et viri spectabiles magistri scriniorum, qui ... qualemcumque divinum responsum dictaverint»), a scribe who gives simple form of the text (*in grossam litteram*) or someone else who affixes the stamp.
2. In general, secretariats, chancelleries and offices come from a different environment. The secretariat refers to a frame that is in closest relationship with the sender, the chancellery is characterized by an institutionalized framework more structured and extra uniform. The offices referred to an operating field with collective senders and structured in skills and public functions (such as for example in the modern states).

Knowing those involved in the document production process is particularly important for diplomats and historians, because this is important for the knowledge of genesis of these documents. And it is this kind of interest especially in diplomatic science, as opposed to other sciences, that also

12 O. Hageneder, *Kanonistiches Recht, Papsturkunden und Herrscherurkunden. Üzu einer vergleichenden Diplomatik am Beispiel der Urkunden Friedrichs* III., in «Archiv für Diplomatik», 42 (1996), p. 422 ss.; Id, *Probleme des päpstlichen kirchenregiments im hohen Mittelalter*, in «Lectiones eruditorum extraneorum in facultate philosophica Universitatis Carolinae Pragensis factae», 4 (1995), pp. 49-77.

deals with the document, but from different perspectives and with different criteria (Palaeography, Literature, History of institutions e.tc.). This happens, because the kind of documents enables scientific regularization and research, since the numerous and diverse written instruments reproduce normally in a given environment almost identical structures.

Bibliography

1. Asonitis, S. N., *Introduction to Latin Diplomacy,* Thessaloniki, 2011. In Greek.
2. Barraclough, G., *Atlante della storia 1945-1975*, Roma-Bari, 1978.
3. Boles, F., *Selecting and Appraising Archives and Manuscripts*, 2nd edition, Archival Fundamentals Series II, Chicago: Society of American Archivists, 2005.
4. Booms, H., *Society and the Formation of the Documentary Herritage: Issues in the Appraisal of Archival Sources* in "Archivaria" I (24) (1987), pp. 9-107.
5. Brandileone, F., *Le così dette clausole al portatore nei documenti medievali italiani* (del 1903), *Origine e significato della "traditio chartae"* (del 1907), *Le così dette clausole al portatore nelle carte di alienazione degli immobili* (s.d.), *Nota preliminare sull'origine della "stantia" o "convenientia"* (del 1923), *La "stipulatio" nell'età imperiale romana e durante il medioevo* (del 1928), in Brandileone, *Scritti di storia del diritto privato italiano*, edit. by G. Ermini, II, Bologna, 1931, pp. 89-146, 59-87, 213-277, 407-418, 419-528.
6. Bresslau, H. and Klewitz, H. W., *Handbuch der Urkundenlehre für Deutschland und Italien*, I, Lipsia, 1912-1932 (rist. Berlin 1958), [in ed. it. : *Manuale di Diplomatica per la Germania e l'Italia*, edit by A. M. Voci-Roth, Roma, 1999 (Pubblicazioni degli Archivi di Stato. Sussidi, 10), pp.721 ss., 842 ss., 861 ss.]
7. Brown, J. S. and Duguid, P., *The Social Life of Information,* Harvard Business School Press, February 2000.
8. Brunner, H., *Zur Rechtsgeschichte der römischen und germanischen Urkunde,* Berlin 1880 (rist. Aalen 1961).
9. Buckland, M. K., *What is a "Document"?* in Journal of American Soci-

ety for Information Science 48 (September 1997).

10. Chabod, F., *Lezioni di metodo storico*, Laterza, Bari, 1969.
11. Costamagna, G., *L' alto Medioevo*, in Amelotti M.– Costamagna G., *Alle origini del notariato italiano*, Roma, 1975 (Studi storici sul notariato italiano, 2).
12. Croce, B., *Teoria e storia della storiografia*, Laterza, Bari, 1927.
13. De Felice, R., *L' archivio moderno nella pubblica amministrazione*, ed. ANAI, Roma, 1969.
14. De Lasala, F. - Rabikauskas P., *Il documento medievale e moderno*, Roma 2003.
15. Duranti, L., *Diplomatics: New Uses for an Old Science*, Lanham, MD: Scarecrow Press, 1998.
16. Hageneder, O., *Kanonistiches Recht, Papsturkunden und Herrscherurkunden. Üzu einer vergleichenden Diplomatik am Beispiel der Urkunden Friedrichs* III., in «Archiv für Diplomatik», 42 (1996), pp.422 ss.
17. Hageneder, O., *Probleme des päpstlichen kirchenregiments im hohen Mittelalter*, in «Lectiones eruditorum extraneorum in facultate philosophica Universitatis Carolinae Pragensis factae», 4 (1995), pp. 49-77.
18. Paoli, C., *Diplomatica*, ed. Sansoni, Firenze 1942, (n. ed.): G.-C.Bascapè in *Manuali di filologia e storia*, serie I, vol. I, Casa editrice Le Lettere, Firenze, 1987.
19. Pratesi, A., *Genesi e forme del documento medievale*, Jouvence, Roma, 1979.
20. Schiaparelli, L., *Note diplomatiche sulle carte longobarde.* III: *La formula "post traditam (chartam)"*. IV: *La formula "post traditam (chartam)" e la "traditio chartae ad proprium" del Chartularium Langobardicum* (del 1933). V: *La formula "sub stipulatione et sponsione interposita"* (del 1934), in Schiaparelli, *Note di diplomatica (1896-1934)*, edit. by A. Pratesi, Torino 1972, pp. 248-301.
21. Steinacker, H., *"Traditio chartae" und "traditio per chartam", ein Kontinuitätsproblem*, "Archiv für Diplomatik", 5-6 (1959-1960), pp. 1-72.
22. Toscano, M., *Storia dei trattati e politica internazionale*, Torino, 1970.

The Cyber Law and Freedom of Expression: The Tanzanian Perspectives

by Damas Daniel Ndumbaro[1]

1. Freedom of expression

Freedom of expression is not only a cornerstone of democracy but also the basis of other rights and freedoms in general. In its very first session in 1946, before any human rights declarations or treaties had been adopted, the United Nations General Assembly (UNGA) adopted resolution stating:

> *"Freedom of information is a fundamental human right and ... the touchstone of all the freedoms to which the United Nations is consecrated."*

The Universal Declaration of Human Rights, 1948, may assist us in giving the more accepted meaning of the freedom of expression. Article 19 of the Universal Declaration of Human Rights says:[2]

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and through any media and regardless of frontiers".*

Not far from that, the Constitution of United Republic of Tanzania, 1977 as amended[3] provides the following on freedom of expression:

> *"Every person*

1 LL.B, LL.M (University of Dar Es Salam, Tanzania), PhD in Law (The Open University of Tanzania), Registered Arbitrator Tanzania Institute of Arbitrators, Advocate of the High Court of Tanzania and Zanzibar, Notary Public & Commissioner for Oaths, Associate Dean and Acting Dean Faculty of Law, Open University of Tanzania.

2 UNGA, Resolution 59(1) of 1946.

3 14th amendment of the Constitution, vide Act of Parliament No 1 of 2005.

(a) has a freedom of opinion and expression of his ideas;
(b) has a right to seek, receive and, or disseminate information regardless of national boundaries;
(c) has the freedom to communicate and a freedom with protection from interference from his communication; and
(d) has a right to be informed at all times of various important events of life and activities of the people and also of issues of importance to the society."

The above two provisions from the above two quoted instruments[4], which are vital to the existence of the freedom of expression, provide that the freedom of expression is all about being free to collect, receive and disseminate news, ideas, opinion and information beyond frontiers. It is about freedom to have and not to be interfered in communications and be informed on the important events and news, both international and local, and freedom to be informed on the matter of importance to people and the community at large. Who has the right and final decision to decide which matter is of importance to the people or community? This is a puzzle, which needs to be undone.

The right to freedom of expression and opinions, the right to seek, receive and impart information and ideas, can only be restricted in certain circumstances. Some of the permitted limitations are related to protection of other rights and reputations of others or protection of national security, public order, public health or morals. Still such a limitation sounds vague and much wider if not properly used by the authority.

It is in record how the freedom of expression has been at the mercy of the authorities discharging statutory duty with wider discretionary powers[5] [6]. Efforts at international and national level record how much free-

4 Universal Declaration of Human Rights 1948 and The Constitution of United Republic of Tanzania, 1977, as amended by Act 1 of 2005.

5 Ndumbaro D.D. *'Decision making and the Law: The Use and Abuse of Discretionary Powers.'* A Paper Presented at the Youth Leadership Training Programme, Dar es Salaam on 24 September 2011. (Unpublished).

6 Discretionary powers are normally legal or statutory powers which are wide in nature and conferred upon an authority to use the same at will or as may deem fit. If you read between the lines in any statute, you may find the clause such as: "may", "deem fit", "in

dom of expression is protected. Johannesburg rules,[7] Camden principles,[8] Article 19[9] etc. are good examples to highlight on the proposed above move to protect and promote freedom of expression.

Professor Gerhard Erasmus[10] offers guidelines for regulating freedom of expression by suggesting that freedom of expression is regulated by human rights, law and violence. On human rights, his argument is straightforward, that, freedom of expression itself is a human right but is not the only one. There are other rights, which need to be respected. In that respect, we may appreciate the usefulness of Article 30 (1) of the Constitution of United Republic of Tanzania, 1977.

On violence, he is establishing a principle that, when human rights and law end, then violence should be used a litmus test for protecting or not protecting freedom of expression. The argument here is: *"the closer the freedom of expression is to the violence, the lesser the protection it is going to enjoy"*. This, in a simple language, means if the freedom of expression is violence in itself or is very close to the violence, there will be little or no protection it is going to enjoy. On law, he simply underlines the usefulness of law in regulating everything, including freedom of expression.

Equally, on the same footing, is the renowned legal and political commentator, Prof. Issa G. Shivji[11], who seems to allow laws to regulate freedom of expression with strong proviso that regulating does not mean eroding. Shivji laments that while trying to regulate the freedom of expression, the statutory instruments or the authorities, go a step further and erode it. Therefore, his problem is not absence of the law to regulate freedom of expression but rather the content of the laws, which regulate the freedom of expression[12].

---

his opinion".

7 http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf. Accessed on 5 May 2016.

8 http://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf. Accessed on 5 May 2016.

9 Ibid.

10 *The Bill of Rights Handbook*. 2nd Ed, Cape Town, Juta & Co. Ltd 1999, 297-322.

11 Shivji GI (2006).

12 Ibid.

1.1 Constitutional provisions

Tanzania has experienced four constitutions since 1961 but it was only in 1984, through amendment to the constitution when the freedom of expression was introduced, together with other rights under the bill of rights. The absence of constitution guarantee and protection occasioned a serious violation of human rights by denying the mechanism for enforcement upon breach. In 1988, the enforcement mechanism of human rights is much more guaranteed in law than any other time in Tanzania. Takrima case[13] of 2006 is also a good reference on the cases on enforcement of bill of rights in Tanzania[14], as in America's Pentagon Papers[15].

The Constitution of United Republic of Tanzania, 1977, as amended, subjects the constitutional rights, including freedom of expression, to the laws of land and other human rights. Article 30 (1) and (2) of the Constitution of United Republic of Tanzania, 1977, insist on respect of other rights and freedom when one exercise his or her rights provided under the constitution or other instruments. The Limitation provided in the above said provision extends also to matters of public interests. The Constitution also, in sub article two of article thirty, insists on the sovereignty of the parliament in enacting laws, which may infringe freedom and rights, including freedom of expression, provided that those laws are intended to; safeguard rights of freedom and rights of others, public interests, public peace, defense, public safety, public morality, public health, development and other matter which is important for the public benefit.

Article 30 of the Constitution of United Republic of Tanzania, 1977, lines up factors such as; others rights[16], defense, public safety, public peace, public morality, public health, authority and independence or authority of the court, confidential information, national interests and enhancement of public benefits as some of the factors which may validly and justifiably makes the freedom of expression not absolute.

13 http://www.commonlii.org/tz/other/TZLRC/report/R11/11.pdf. Accessed on 8 January 2016.

14 Ibid.

15 http://www.u-s-history.com/pages/h1871.html. Accessed on 18 November 2016.

16 Which includes: Reputation, Freedom, Privacy and Dignity?

1.2 International and regional legal instruments

International and regional legal instruments, alternatively called agreement, convention, covenant, treaty, protocol etc., bind contracting states to the negotiated terms. When negotiations are completed, the text of a treaty is established as authentic and definitive and is signed by the representatives of states. A state can agree to be bound to a treaty in various ways. The most common are ratification or accession. A new treaty is ratified by those states that have negotiated the instrument. A state that has not participated in the negotiations may, at a later stage, accede to the treaty. The treaty enters into force, or becomes valid, when a pre-determined number of states have ratified or acceded to the treaty.

As early as 1946, at its very first session, in the UN General Assembly adopted Resolution 59(I) which states: "Freedom of information is a fundamental human right and ... the touchstone of all the freedoms to which the United Nations is consecrated." This has been echoed by other courts and bodies[17]. The European Court of Human Rights has recognized the vital role of freedom of expression as an underpinning of democracy when the court remarked: "Freedom of expression constitutes one of the essential foundations of [a democratic] society, one of the basic conditions for its progress and for the development of every man."[18]

At international and regional level, there are several instruments, which support and cement the freedom of expression[19]. According to several inter-

17 For example, the UN Human Rights Committee said: "The right to freedom of expression is of paramount importance in any democratic society".

18 *Handyside v. United Kingdom*, 7 December 1976, Application 5493/72 para 49.

19 African Charter of Peoples and Human Rights (ACPHR), 1981; Camden Principles on Freedom of Expression and Equality, 2009; Convention of the Rights of the Child (CRC), 1989; Convention on the Elimination of All Forms of Discrimination Against Women August (CEDAW), 1979; Convention on the Rights of the Child (CRC), 1989; Declaration of Principles on Freedom of Expression in Africa, 2002; European Convention on Human Rights (ECHR), 1953; International Convention on Civil and Political Rights 1966; International Convention on Civil and Political Rights (ICCPR), 1966; International Convention on the Elimination of All Forms of Racial Discrimination (ICEFRD), 1965; International Covenant on Civil and Political Rights (ICCPR), 1966; Johannesburg Principles on National Security, Access to Information and Protection of the Source, 1996; Mozambique Constitution, 1990; Singapore Declaration on Hu-

national instruments, everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Effective information systems that allow free flow of information are always key to enhance democracy, accountability and respect for human rights.

International and national bodies and courts worldwide have insisted and demonstrated also that the right to freedom of expression is central to the international human rights regime and human dignity. That may be the case because all the greatest man-made calamities that have plagued the world for centuries, were caused by expressions, opinions and at time conscience[20]. It is an instrument to assist in the attainment, preservation or continuance of somebody's power, whether exercised by an individual, an institution or a state. It is the extension of physical power into the realm of the mind and the spirit….[21]" Therefore the abuse or misuse of freedom of expression may plunge the country into a man-made calamity.

1.3 Constitutional provisions and freedom of expression

Freedom of expression is also guaranteed by Article 18 of the Constitution of the United Republic of Tanzania of 1977. The Constitution provides that everyone has a right to give his or her opinion and receive any information of public interest and pertinent to the welfare of the nation. However, freedom of expression and the right to information in Tanzania

man Rights, 1993; United Nations General Assembly Resolution No. 59 (1),14th December 1946; United Nation Special Rapporteur on Freedom of Opinion and Freedom of Expression, 1959; United National General Assembly Resolution (UNGA), No. 217A(111) 1948; Universal Declaration of Human Rights (UDHR), 1948; The Declaration of the Right of the Man and Citizen, 1789; The African Charter on the Right of the Child 1990; American Convention on Human Rights, 1969; Declaration on the Human Rights of Individuals who are not Nationals of the Country in Which They Live 1985; The European Convention for Protection of Human Rights and Fundamental Freedoms, 1950; and Yaounde Declaration, 1981.

20 The slave trade, slavery, the inquisition, the Holocaust, the Genocide in Cambodia and Rwanda are examples.

21 Michael Scammell, 'Censorship and its History – A personal View', *Article19 World Report* 1988, 5.

are not fully enjoyed because of several reasons such as lack of specific legislation protecting these rights, draconian freedom of expression laws, related legislation and the misuse of power by state officials.

Despite the legal framework above, access to information in Tanzania is still a critical problem. The right to information among other things is curtailed by existing bureaucratic systems, legal systems, poverty, high level of ignorance and existing governance system. The most affected part of the community is those in the rural set up[22]. The 2012 MISA-Tan report indicate that access to information is still a major challenge in Tanzania[23].

1.4 Internet access

Tanzania has witnessed the growth in terms of quantity and quality of some indicators of freedom of expression such as media, associations, political parties, forums, demonstrations, strikes etc. Some of the indicators like media have grown up in number[24] but the law is still the same. There must be a force behind such a growth because the media laws have remained static but the changes in media industry are noticeable.

Freedom of the press in particular, has long been considered crucial to democracy, human rights and development because the news media provide a fundamental informational linkage between the government and the mass publics. For media consumers, freedom of the media is defined as freedom to consume information or entertainment from any source without government restrictions.

Internet access was mainly an urban centered affair because of the lack of computers, electricity and network connectivity in the rural areas where

22 LHRC Annual Report 2013.

23 (MISA-Tan surveyed 8 government institutions and measured the levels of openness and secrecy. Selected institutions and Ministries were the Ministry of Finance; The National Housing Corporation (NHC); the Tanzania Electric Supply Company Ltd (TANESCO); Tanzania Revenue Authority (TRA); Ministry of Works; Tanzania Commission for Aids (TACAIDS). Others were Surface and Marine Transport Regulatory Authority (SUMATRA) and the Ministry of Legal and Constitution Affairs).

24 MCT (2012), MISATAN (2012), and National Information Services (MAELEZO 2012), 68 newspapers and 644 other publications 28 television stations and 59 radio station registered. See also Shivji G *Let the People Speak, Tanzania Down the Road to Neo Liberalism*. Dakar, CODESRIA 2006.

majority of Tanzanian are located. The trend has changed now with the coming of the mobile telephone companies[25] providing both voice and data services which make internet access possible. With the increase of the use of the mobile transaction, the question of cybercrime is no longer a remote issue.

Internet service providers are subject to the Electronic and Postal Communications Act[26], and its regulations as well as the new Cybercrime Act, 2015. The courts in Tanzania are yet to test the applicability of the defence such as mere conduit or common carrier which are basically essential for protection of cyber operator/service provider. With the exponential increase of online transactions through mobile phones, the role of the court and applicability of this possible defence will much more evident.

2. Criminalization of freedom of expression

The freedom of expression laws in Tanzania can basically be grouped into three facets; First, the Constitution[27] and other international instruments on freedom of expression[28] and Acts of Parliament[29]. Second the laws specifically enacted to regulate the media profession such as, the Newspaper Act[30], Tanzania Broadcasting Services Act[31], Tanzania Communication Regulatory Act[32], Electronic and Postal Communications Act[33], e.tc. Third, laws made for other purposes but in one way or the other regulate the freedom of expression[34]. The list of other laws made for other purpose but in one way or the other regulates or control freedom of expression is long and

25 TTCL, Vodacom, Celtel, Tigo, Sasatel, Halotel. 32 million people use mobile phone in Tanzania;https://www.google.co.tz/#q=number+of+mobile+phone+subscribers+in+tanzania, accessed on 15th February 2016.

26 Act No. 3 of 2010.

27 The United Republic of Tanzania, 1977 as amended.

28 Universal Declaration of Human Rights, 1948.

29 International Broadcasting Standards.

30 Cap 229 of the Laws of Tanzania RE 2002.

31 Cap 306 of the Laws of Tanzania RE 2002.

32 Act 8 of 2003.

33 Act No. 3 of 2010.

34 National Security Act, Prison Act; Prevention of Terrorism Act, etc.

may take more take to discuss them[35].

3. Cyber freedom and the wrath of the laws

There is no doubt that cybercrimes are a threat to the national security and other individual's rights enjoyments because cybercrime is unlawful acts wherein the computer is either a tool[36] or a target[37] or both.

The history of the cybercrime is dated as far back as 1820 though the most notable one was the first spam mail, which happened in 1976, and the first virus was installed in 1982[38]. The history of statutory regulation of cyber transactions has been an up and down phenomenon for many countries. In US, for example, the struggles between the First Amendment supporters, on one hand and children on-line Protection, on the other hand cannot be ignored[39]. While we all appreciate the wideness and wildness, which the cyber freedom has brought to us, we are mindful also on the need to regulate the same in order to protect other rights and values in the society.

35 Newspapers Act of 1976; Tanzania Broadcasting Services Act, 6 of 1993 (Cap 306 RE 2002); Films and Stage Plays Act, 1976; The Tanzania Communications Regulatory Authority Act 12 of 2003; Tanzania Revenue Authority Act 11 of 1995; Penal Code, Cap 16; Records and Archives Management Act 3 of 2002; Regional Administration Act 19 of 1997; The Prisons Act 34 of 1967; and Public Leadership Code of Ethics Act 13 of 1995. Others include; Public Leadership Code of Ethics Act 13 of 1995; Tanzania News Agency (Repealing) Act 2000; Local Government (District Authorities) Act, 1982; The Police Force and Auxiliary Forces Act 1 of 1987; The Tanzania Library Services Act 6 of 1975; The Standards Act 3 of 1975; The Privatization Trust Act 7 of 1997; The Tanzania Communications Act 18 of 1993; and The Customs (Management and Tariff) Act 2 of 1952 (Cap 27 RE 2002); The Income Tax Act, 2004; The National Security Act 3 of 1970; The General Loan and Stock Act 21 of 1948 (Cap 255 RE 2002); The Statistics Act 1 of 2002 (Cap 351 R.E 2002); The Petroleum (Exploration and Procurement) Act 27 of 1980 (Cap 328 RE 2002); The Mining Act 5 of 1998 (Cap 123 R.E 2002); The Evidence Act 6 of 1967 (Cap 6 RE 2002); and The Fair Competition Act 4 of 1994 (Cap 285 RE 2002); CyberCrime Act, 2015; Electronic and Postal Communications Act, No. 3 of 2010.

36 Using a computer to commit real world crime e.g., cyber terrorism, credit card fraud and pornography.

37 Using a computer to attack other computer e.g. hacking, virus/work attacks, etc.

38 Rich Skrenta, the High School Student, developed *EIK Cloner.*

39 Doug Isenberg, Giga law.

On April 1 2015, the Tanzanian parliament passed a cybercrime law that attempts to address child pornography, cyber bullying, online impersonation, electronic production of racist and xenophobic content, unsolicited messages (i.e. spam), illegal interception of communications, and publication of false information — all in one law. The Cybercrime Act[40] guarantee freedom of expression through Internet but only within the scope and framework prescribed under the statute. There are restrictions on the accessibility to freedom of expression, which need to be gauged against the international standards.

Notable features of the cyber law in Tanzania is not only the non involvement of stakeholders during the enactment process but also the support which the law received in the parliament from both the ruling party and oppositions members of parliament. The support is based on the arguments that the law guarantee protection against: Child Pornography, Incitement to commit suicide, Racist Materials, invasion of the privacy, illegal access, illegal interception, data interference, system interference, misuse of devices, forgery, fraud, offences related to child pornography, identity theft and other most serious crimes on social networks of global concern.

The supporters further argue that, the recently introduced Cybercrime Act of 2015 by the parliament of Tanzania promises to provide security to all citizens from any sort of cyber-attack that may come their way as they are surfing on the Internet. For a developing country like Tanzania this is a big step in trying to make sure justice is served and that all those that are using the internet as a medium to take advantage of people's rights, privacy and that of the state are dealt with accordingly.

A report by the Tanzania Communication Regulatory Authority (TCRA)

40 Act No. 4 of 2015 of Tanzania. The law applies both in Tanzania mainland and Zanzibar, has 59 sections which among other things, create several computer related offences and amend other four laws, namely; The Electronic and Postal Communications Act; the Penal Code making destruction of any device which contains evidence a crime; The Anti-Money Laundering Act; and Extradition Act by inserting the words cybercrime in offences under the said statutes, making it an offence under the Anti-Money Laundering Act and an extraditable offence. It should be noted that, the Act confers jurisdiction to convict any Tanzanian citizen within or outside the country or a foreigner within or outside the country if this foreigner committed a crime against a person located in Tanzania.

shows that Internet services in Tanzania commenced from the year 1995 and it has been exponentially growing[41]. This growth shows that Tanzanian currently depend on the wind of info-technology, in healthcare, transport and most especially for communication. Technology has made life much easier than it was before, in every sense. There are now several websites that can help one get any product or service simply by the click of a button.

E-commerce in Tanzania is growing fast due to the increasing number of Internet users and service providers in the country. The country is at a stage where it is vital that its people feel secure when buying products or booking tickets through the Internet via websites like Kaymu or Travel start[42].

The law is a sign that Tanzania as a developing country is heading in the right direction, like other European and western countries already has; this is a positive step that the country is taking in catching up with the rest of the world. With the new law, using the Internet will very much be more enjoyable and comfortable and additionally problems associated with Internet scams can be dealt with accordingly and all those who are responsible for misconduct, will be punished as required[43].

The other side of the argument forcefully and vigorously criticizes the laws for overstepping the boundary and being draconian. The law, they argue covers much more than serving the legitimate purposes. The Parliament passed the law and the president assented it despite criticism from social media practitioners and human rights activists[44]. One of the critiques was the then Deputy Minister of Science and Technology, Honourable January Makamba, MP, who tweeted:

"I am worried about the power given to our police. Ignorant and low

41 There has been a steady growth of internet users from 3.5million people in 2008 to over about 11 million out of the 32 million Tanzanians with access to mobile phones by the end of 2015.

42 www.kyumu.co.tz.

43 Mr. Richard Maguluko, one of the Tanzanians with online shopping experience, tells us his thoughts on cybercrime, "In the recent years we Tanzanians have been hesitant in using E-commerce sites because there are a lot of conmen out there trying to deceive the citizens and they get away with it many times."

44 http://www.cipesa.org/2015/04/tanzania-cyber-crime-bill-should-safeguard-citizens-rights-on-the-internet/.

income earners might suffer"

The worry of the Honourable Deputy Minister is founded on the facts that the law gives police wide ranging ability to search the homes of suspected violators of the law, seize their electronic hardware, and demand their data from online service providers[45]. The worry on powers given to police was vivid during the 2015 Presidential General Election whereby police searched and seized computer, cell phones and other electronic gadgets of opposition party[46] and human rights organization[47] that was monitoring the election.

EPOCA[48], though, did not catch the attention of the critiques when enacted, deals with Cyber-security, Interception, Encryption and Data Retention, which are key factor in the cyberworld. When a law enforcement agent requires the information[49], the court of law or other judicial body that needed information must be submitted to the relevant authority, thereby compromising the privacy of the consumers of freedom of expression. The situation is compounded by lack of Data Protection legislation[50].

The state can equally intercept communication of an individual by making an application to the public prosecutor for authorization to intercept or to listen to any communication transmitted or received by any communications. The public prosecutor must consider whether any communications is likely to contain any information, which is relevant for the purpose of any investigation into an offence before authorizing such access.

45 Aidan Eyakuze and Ben Taylor, both of whom work for the independent East African initiative TWAWEZA.

46 Chama cha Demokrasia na Maendeleo (CHADEMA).

47 Legal and Human Rights Centre. (LHRC).

48 Electronic and Postal Communications Act, No. 3 of 2010.

49 Police, Security services, Regulatory authority, etc.

50 Electronic and Postal Communication Act regulations on consumer protection state that a licensee may collect and maintain information on individual consumers where it is reasonably required for its and lawfully collected and processed. Processed for identified purposes. Accurate. Processed in accordance with the consumer's other rights. Protected against improper or accidental disclosure. Not transferred to any party except as permitted by any terms and conditions agreed with the consumer as permitted by any approval of the Tanzania Communications Regulatory Authority or as otherwise permitted or required by applicable laws and regulations.

EPOCA has 44 sections establishing different offences, which criminalize freedom of expression and create a harsh environment for one to enjoy the much-needed freedom of expression[51]. The law has criminalized the transmission of obscene communications[52] but there is a lack of clarity on what is obscene under the law and other statutes. An uncertain law such as this is like walking in the land mine during the night, with very high probability of casualties.

The other negative side of the law punishes the anyone who uses a cyber network without authorization as it is spelt in section 124 (30 of the Electronic and Postal Communications 2010 Act:

> *"124.- (3) Any person who secures unauthorized access to a computer or intentionally causes or knowingly causes loss or damage to the public or any person, destroy or delete or alter any information in the computer resources or diminish its value or utility or affect it injuriously by any means, commits an offence and on conviction shall be liable to a fine not less than five hundred thousand Tanzanian shillings or to imprisonment for a term of not exceeding three months or to both".*

The challenge is when an access is deemed to be authorized and when is deemed to be not authorize? Further who authorizes the access and in case of refusal of authorization what are the available legal remedy? The discretionary powers vested to the authority to allow of refuse access without assigning any reasons and failure of the law to provide remedial measures is a bottleneck to the enjoyment of freedom of expression.

The Electronic and Postal Communications Act[53], further criminalize what it calls "false information" in the following manner:

> *"s. 132. Any person who furnishes information or makes a statement knowing that such information or statement is false, incorrect or misleading or not believing it to be true, commits an offence and shall be liable on conviction to a fine of three million Tanzanian shillings or*

51 Part VI, sections 116-160 of the Electronic and Postal Communications Act No. 3 of 2010.

52 S. 118 of the Electronic and Postal Communications Act No. 3 of 2010.

53 Section 132 of the Electronic and Postal Communications Act, No. 3 of 2010.

to imprisonment for a term of twelve months or to both".

Twelve months imprisonment or Three Million Shillings fine (US$ 1500) or both is such a harsh statement for someone who is alleged to have published false information is an impediment to the freedom of expression. The challenges on what is false information is not answered under the law, thereby making it a fertile ground for abuse of freedom of expression.

It is evident from the above arguments and counter arguments that the cybercrime statute has got both supporters and opposers, each camp having equally strong arguments. Critical and impartial analysis of the law and its applicability in Tanzania will perhaps, give us the real and uncontaminated position of the law.

4. Critical assessment of cyber laws, freedom of expression and intellectual property in Tanzania

I join hands with those who support the Cybercrime Act on three facets: child pornography, incitement to commit suicide and racist materials because these are permissible restrictions under international and regional instruments on freedom of expression.

I profound differ with them when these laws seem to accommodate other non-permissible restrictions such as data espionage[54] because data which have been restricted to be accessed under section 8 of the Cybercrime Act, may be a piece of information which is critical for investigative journalism, research or other legitimate use. Restricting it is restricting freedom of expression and it cannot pass the international standards on freedom of expression.

While the law is credited for prohibiting child pornography, it is criticized for unnecessarily curtailing freedom of expression by prohibiting pornography[55]. Pornography is different from child pornography. The former is a free choice of an matured adult and is not prohibited under international standards on freedom of expression, thus section 14 of the Cybercrime Act, has overstepped the line for trying not only to impose un

54 S. 8 of the CyberCrime Act, 2015.
55 Section 14 ibid.

acceptable restrictions but also by criminalizing freedom of expression.

The talk of the country was on section 20 of the Cybercrime Act, 2015 which reads:

20.-(1) A person shall not -

(a) Initiate the transmission of unsolicited messages;

(b) relay or retransmit unsolicited messages , or

(c) falsify header information in unsolicited messages.

2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or three times the value of undue advantage received, whichever is greater or to imprisonment for a term of not less than one year or to both.

(3) For the purpose of this section, "unsolicited messages" means any electronic message, which is not solicited by the recipient.

Certainly this is one of the most debated provisions of this law. Initially there was an unfounded belief that even a recipient of the unsolicited message is guilty under section 20 above but a close look at it reveals otherwise. The recipient will only be liable if he or she relay or modify the content in a bid to falsify it[56]. There are two angles on which one may analyze the provision of the law above. One, at what point in time a message becomes unsolicited? What if the message is very much needed and critical to my survival but I did not solicit it, should the transmitter be punished for assisting and perhaps serving my life? Obviously, the law brings more questions and criticisms than answers and solutions.

Further, section 20 (2) of the Cybercrime Act 2015, leaves much to be desired in terms of punishment for unsolicited messages. The first option is either a fine of Tanzanian Shillings Three Million Only (equivalent of US$ 1500) or three times the value of undue influence gained whichever is greater. A fine of United Dollars fifteen Hundred is a lot of money for a common Tanzanian, even for middle-income earner. Three times the value of undue influence brings more uncertainty. The uncertainty is a fertile ground for

56 Section 20 (1) (a) & (b) ibid.

abuse and misuse of the law. A critical issue to be taken into consideration is who decides on the three times the value of undue influence? As if that is not enough, the above provision provides a further option of a minimum of one year behind the bar as alternative to the fine but sometimes both, one can pay a fine and still go to prison. A sentence can thus be even 20 years with a fine of six figures in United States Dollars. Obviously, such harsh, subjective and uncertain punishment is a fertile ground for abuse and misuse of law, which brings chilling effects in the society and suffocates freedom of expression.

Publication of false, deceptive, misleading, or inaccurate information, data or facts is one of the offences[57] which not only curtails the freedom of expression but also has been put into a practice than any other provision of the law. Section 16 of the Cybercrime Act, 2015, is a replica of News Papers Act[58], which was, in 1992, declared unconstitutional by the Nyalali Commission[59]. Most of the targeted information, data and facts, under this provision of the law are from political elections[60]. All the cases arise from section 16 of the cyber law but we can discuss much about the cases because they are sub-judice. This is mousetrap for bloggers, what sup and online media.

Part iv of the law deals with search and seizure. A police officer in charge of the police station or any law enforcement officer may search and seize cell phones, computer, ipads, notice or any device. These search and seizure powers given to police were criticized even by the Deputy Minister[61] for being not only wide but also a recipe for abuse. The criticisms were more realistic during the Presidential General Elections 2015 where opposition parties and Legal and Human Rights Centre offices were searched and computers, cell phones and other electronic gadgets were seized.

Protection of the source is one of the cardinal principles of media pro-

57 Section 16 ibid.

58 Act No. 3 of 1976

59 Chaired by former Chief Justice, Francis Nyalali, the commission recommended the repeal, among other laws, the News Papers Act.

60 There are four pending cases at Resident Magistrate Court of Dar Es Salaam, at Kisutu: *Republic vs. George Aloyce Kimaryo; Republic vs Yerickp Yohanessy Nyerere; Republic vs Leila Constatine Sinare* and three others.

61 January Makamba, supra.

fession. A source is a fountain of freedom of expression, thus if we want to promote freedom of expression, the law should always guarantee the protection of the source. There is less debate on protection of the source in other professions such as doctor-patient; lawyer-client; banker-customer but when it comes to the media profession, there is more unjustifiable reluctances. This is evident under section 36 of the Cybercrime Act, 2015 where the laws compels anyone to disclose whatever information is needed by the law enforcement officers. May mean disclosure of the source for the media and intrusion of privacy.

Violation of intellectual property rights through internet has been discussed under the Cybercrime Act[62] whereby a person is not allowed to use the internet to violate intellectual property protected under any written law. While it is good to legally protect intellectual property, the same acts should not violate freedom of expression.

Human rights activists filed a case at the High Court, protesting some sections of the Cybercrime Act, September 2015. The Tanzania Human Rights Defenders Coalition (THRDC), Legal and Human Rights Centre (LHRC) and other organizations filed a petition as a complainant, seeking the amendment of some sections, which are "threats to free and open expression online". The challenged provisions are: Sections 31,33,34,35 and 37 which give powers to police to search users of online data in the absence of a court order, thus contradicting Article 16 of the constitution. Until now the matter is *sub-judice.*

5. Conclusion and recommendations

The Cybercrime Act, 2015, therefore, can be viewed and discussed in the following facets: It duplicates offences from other laws; It criminalizes and drawbacks freedom of expression, especially online media; it applies beyond the media; and it violates international standards on freedom of expression. The law further provides a possibility of someone being charged and ultimately punished twice for the same offence under different and other laws the Newspapers Act of 1976. This creates a window shopping of justice.

62 Section 24 of the Cybercrime Act, 2015.

The process towards the enactment of the law was exclusive instead of being inclusive. The involvement of stakeholders is critical in any meaningful law making process. In so doing, attention should be paid to the need to respect international standards on freedom of expression, allow freedom, which is cornerstone of democracy, to take its course. Access to the internet is a human right, thus any attempt to regulate it should be in total compliance to the international regulations.

The Cybercrime Act needs to respect the Constitution of United Republic of Tanzania, 1977, as amended and other International Instruments on freedom of expression such as the International Covenant on Civil and Political Rights, African Charter on Human and Peoples Rights, Commission on Human and Peoples Rights, African Court of Human and Peoples Rights, etc.

6. References

1. Konde, H.S. (1984) Press Freedom in Tanzania Arusha: East Africa Publications Limited.
2. LHRC and ZLSC, (2013) Tanzania Human Rights Report 2012, Dar es Salaam: LHRC and ZLSC.
3. Maugo, W. 'A veteran editor speaks: Facts and myths about editorial freedom'. In White, A. (2012) (ed.) African Communication Research vol. 5, no. 1, 115-126 Mwanza: SAUT.
4. MCT, (2008) State of Media Report 2007 Dar es Salaam: MCT.
5. MCT, (2013) State of Media Report 2012 Dar es Salaam: MCT.
6. Misatan, (2012) Government Secrecy in an Information Age: Report on Access to Mtambalike, P. "From Press Freedom to Media Responsibility: The Role of Self Regulatory Bodies" A paper presented at Regional Seminar on Media Law and Ethics, March 27-30, 2008 Nairobi: Media Council of Kenya.
7. Mwakyembe, H. (1998), 'Media Boom, Media Freedom and the Legal Environment in Mainland Tanzania' Lesotho Journal of Law vol. 2, no. 2, 1998 Maseru: National University of Lesotho.
8. Ndumbaro D.D. 'Decision making and the Law: The Use and Abuse of Discretionary Powers.' A Paper Presented at the Youth Leadership

Training Programme, Dar es Salaam on 24 September 2011 (Unpublished). On file with the author.

9. Ndumbaro, D.D. 'The Impact of Globalization o on Freedom of Expression and Media Laws in Tanzania' unpublished PhD thesis, Open University of Tanzania, 2013.
10. Nyamnjoh, F.B. 'Media Ownership and Control in Africa in the Age of Globalization' In Rioba, A. (2012) Media Accountability in Tanzania's Multiparty Democracy: Does self regulation works? Tampere: University of Tampere.
11. Rioba, A. (2008) Media Ethics. Dar es Salaam: The Open University of Tanzania.
12. Scammell, M. (1988) 'Censorship and its History: A personal View' London: Article 19.
13. Shivji, I.G. (2006) Let the People Speak; Tanzania Down the Road to Neo Liberalism Dakar: CODESRIA.
14. Shoo, G. (2002) The New Press Bills in Tanzania: Implications for National Communication Policy and Press Freedom African Media Review vol. 11, no. 2, 2002.
15. Sturmer, M. (1998) Media History of Tanzani, Songea: Ndanda Mission Press.
16. The Constitution of the United Republic of Tanzania, (1977) 2005 revision Dar es Salaam: Government Printer.
17. White, A. 'The need for the Dar es Salaam Declaration of Editorial Freedom, Independence and Responsibility' In White, A. (2012) (ed.) African Communication Research vol. 5, no. 1, pp. 5-8 Mwanza: SAUT.

Behind a Veil of Obscurity – Anonymity, Encryption, Free Speech and Privacy

Christoph Bezemek[1*]

1. The Scoundrel's Letter

When I was a senior in high school I had a wonderful history teacher; knowledgeable, open-minded and critical when it came to his subject and the methods employed in order to grasp it. I lively do remember, for example, one episode in class, when we were discussing a letter to the editor of a newspaper published just the very day in the paper's morning edition. I have to admit that I have no recollection whatsoever of the letter's content (which, of course, makes this effort of story-telling rather miserable). But I do recall that it was an anonymous letter we were talking about. As well as I do recall what my teacher told us about this way of conveying one's views: "only scoundrels", he said, "write anonymous letters".

And, of course his position seemed to be perfectly comprehensible. And why shouldn't it be? Indeed, public discourse as a democratic society's

1 * Associate Professor, Institute for Austrian and European Public Law (IOER) WU (Vienna University of Economics and Business), Welthandeltsplatz 1, D3, 1020 Vienna, Austria, christoph.bezemek@wu.ac.at

The following essay was drafted as a contribution to the 7th International Conference on Information Law and Ethics, held at the University of Pretoria, South Africa on Feb 22 and 23 2016. Honoring the conference title, "a time for inclusion", rather than focusing on a specific national legal system, it contains a fundamental rights collage, primed by some general considerations, and draws on some international examples that may illustrate the problems to be solved. Some of the thoughts introduced here were originally developed, however, for a lecture at the First General Assembly of the MAPPING (Managing Alternatives for Privacy, Property and Internet Governance) project in Hannover on Sep 23 2015, where I was asked to discuss the question 'Do the Fundamental Rights to Privacy, Freedom of Press and Freedom of Expression (now) entail a right to anonymous/encrypted communication?'. I would like to thank Maria Botti und Nikolaus Forgó for their kind invitations to speak at these events, the participants for lively discussions and most helpful suggestions and my history teacher, Wolf Peschl, of course, for many valuable lessons.

bonding agent, creating "a public communicative sphere by making common experiences available to those who would otherwise remain unconnected strangers",[2] desperately is in need of men and women who speak their minds freely without taking refuge behind a veil of obscurity. At its foundation rests an understanding of "civic courage", as Louis Brandeis famously put it in Whitney v. California, "to be the secret of liberty";[3] courage that asks to stand behind one's convictions, in particular when the majority of the community holds different views and even though repercussions are to be expected. A democratic Society, to sum it up, cannot exist without the likes of Emile Zola, openly shouting out their 'J'Accuse' at public grievances and abuses of power.[4]

2. An Honorable Tradition

I still hold this to be true, and yet, many arguments as brief as the one I just presented may well have their share of truth, while being still too simple**:** The basic willingness of its citizens to stand up and to stand out, may be a necessary precondition of any society to be called democratic; but even assessed from the perspective of a free speech principle, it certainly is not a sufficient one, which from the very outset disqualifies the perception of all those who choose alternative ways to spread their views as 'scoundrels'. History, of all disciplines, proves best to what great extent anonymity in public discourse and democratic structures are interrelated and identifies "anonymous pamphleteering not [as] a pernicious, fraudulent practice, but

2 Robert Post, Recuperating First Amendment Doctrine, 47 Standford Law Review 1995, 1249 (1276). Also see Robert Post, The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine v. Falwell, 103 Harvard Law Review 1990, 601 (635), and, in general for the concept of the public sphere, the seminal analysis by Jürgen Habermas, Strukturwandel der Öffentlichkeit (1962).

3 Whitney v. California, 274 U.S. 357 (1927) 375 (Brandeis, J. concurring).

4 Le Figaro, 13 January 1898. See Henri Guillemin (ed), Émil Zola, J'accuse! La vérité en marche (Éditions Complexe 1988) 97-113. For a recent contribution on how Zola's intervetion helped to shape the modern understanding of the public intellectual Steve Fuller, The Public Intellectual as Agent of Justice: In Search of a Regime, 39 Philosophy and Rhetoric 2006, 147.

[as] an honorable tradition of advocacy and of dissent":[5]

It is hard, for example, to imagine the longing of the British colonies in America for independence without Thomas Paine's famous pamphlet on 'Common Sense' coming to one's mind, originally published anonymously in the first and then as written "by an Englishman" in the second edition.[6] And it is hard to imagine the formation of the United States without the Federalist papers, 85 essays written by Alexander Hamilton, James Madison and John Jay under the pseudonym 'Publius' promoting the ratification of the Constitution.[7] The same holds true for the letters critical of the government of King George III published under the pseudonym 'Junius' in the pages of the 'Public Advertiser' in 18th century England,[8] it applies to Voltaire's 'Candide',[9] arguably to the works of William Shakespeare,[10] and countless further accounts on this side or the other side of the Atlantic that significantly influenced public discourse and eventually altered the political landscape. And they did so behind the aforementioned veil of obscurity. Or perhaps better: these influences may never have come to light and these alterations may have never happened, was it not for the veil of obscurity behind which advocacy could take refuge: either to allow the argument instead of the writer to come to the fore,[11] thereby overcoming

5 McIntyre v. Ohio Elections Comm'n 514 U.S. 334 (1995) 357.

6 Common Sense; Addressed to the Inhabitants of America (both editions Bell 1776). The addition to the second edition was made, however, by Bell without Paine's consent – cf. Alfred Aldridge, Thomas Paine's American Ideology (1984) 42. Generally, for the 'Republican Charisma' exemplified by Common Sense see J. Michael Hogan/Glen Williams, Republican Charisma and the American Revolution: The Textual Persona of Thomas Paine's Common Sense, 86 Quarterly Journal of Speech 2000, 1.

7 For the First Collection of these Essays originally published between 1787 and 1788 in the New York Packet, The Daily Advertiser and The Independent Journal cf. the Federalist: a collection of essays written in favor of the new Constitution as agreed upon by the federal convention, September 17, 1787. In Two Volumes (Mc Lean 1788). On the question of the authorship of the respective essays see Jacob E. Cooke, The Federalist (1961) xix-xxx.

8 For the First (authorised) Collection of the letters originally published in the ‚Public Advertiser' between 1769 and 1772, cf Junius: Stat Nominis Umbra (Woodfall 1772).

9 Candide ou l'Optimisme, Traduit de l'Allemand de Mr. le Docteur Ralph (1759).

10 See, for a recent encunter with the topic, James Shapiro, Contested Will: Who Wrote Shakespeare? (Simon and Schuster 2010).

11 See, on the question of 'source-bias' i.a., Chesa Boudin, Publius and Petition: Doe v.

possible trenches of partisanship and personal prejudice,[12] or to highlight the author's position by the use of a certain pseudonym,[13] or, perhaps typically, because the ideas expressed were considered subversive, treacherous or blasphemous; too dangerous in any case to be freely circulated among the public.

Focusing on the last element, it is safe to state, as Hugo Black did for a US Supreme Court majority in Talley versus California, that "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind;"[14] as on many occasions, anonymity proved to be an essential tool for speaking truth to power. Sadly in many places it still is.[15] Yet, even where it is not, in the democratic societies adhering to the rule of law many of us have the privilege to live in, "[a]nonymity [serves as] a shield from the tyranny of the majority. [And as such it indeed and in manyfold ways does] exemplify the purpose of [fundamental rights in general and of freedom of speech] in particular: to protect unpopular individuals from retaliation-and their ideas from suppression-at the hand of an intolerant society."[16] We may, therefore, conclude by referring to Catalina Botero Marino, then Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights: "[t]he protection of anonymous speech is conducive to the participation of individuals in

Reed and the History of Anonymous Speech, 120 The Yale Law Journal 2011, 2140 (2155-2156).

12 A point of particular importance during the ratification of the US Constitution – see Victoria Smith Ekstrand & Cassandra Imfeld Jeyaram, Our Founding Anonymity: Anonymous Speech during the Constitutional Debate, 28 American Journalism 2011, 35 (45-47, 49-52). Also see Eran Shalev, Rome Reborn on Western Shores: Historical Imagination and the Creation of the American Republic (2009) 158 and Robert G. Natelson, Does "The Freedom of the Press" Include a Right to Anonymity? The Original Meaning, 9 New York University of Law & Liberty 2015, 160 (184-185).

13 See, e.g. for the Amercian Revolution Arthur Schlesinger, Prelude to Independence: The Newspaper War on Britain 1764-1776 (Kopf, 1958).

14 Talley v. California 362 U.S. 60 (1960) 64.

15 See for a recent contribution Helmi Norman, Arab Religious Skeptics Online: Anonymity, Autonomy, and Discourse in a Hostile Environment, The Berkman Center for Internet & Society at Harvard University, Research Publication No. 2015-2, February 4, 2015.

16 McIntyre v. Ohio Elections Comm'n 514 U.S. 334 (1995) 357.

public debate since—by not revealing their identity—they can avoid being subject to unfair retaliation for the exercise of a fundamental right."[17]

3. … and the Press

Of course, it is not only individuals, acting independently based on their free-speech claims that beneficially employ anonymity in conveying their messages without having to fear the powerful forces they may be directed at. Anonymity has traditionally (and correctly) been perceived as essential prerequisite of the press and other media to assume their role of what the European Court of Human Rights calls a "public watchdog",[18] guarding the public interest as a turning table of information: To a lesser extent as far as anonymous reporting is concerned, for which there are, at least nowadays,[19] few, however relevant examples - think of the British weekly "The Economist"; to a far greater extent as far as journalistic sources are concerned. As the ECtHR emphasized in Goodwin v. UK, its leading case on the subject: "Protection of journalistic sources is one of the basic conditions for press freedom […]. Without such protection, sources may be deterred from as-

17 Catalina Botero Marino, Freedom of Expression and the Internet (2013) § 134.

18 ECtHR 25.3.1985, Barthold v. Germany, 8734/79 § 58 and for the Court's more recent case law 8.12.2015, Caragea v. Romania, 51/06 § 26. The Court's case law, however, keeps expanding the attribution of "watchdog" as "the function of creating forums for public debate is not limited to the press. That function may also be exercised by non-governmental organisations, the activities of which are an essential element of informed public debate. The Court has therefore accepted that non-governmental organisations, like the press, may be characterised as social "watch-dogs". In that connection their activities warrant similar Convention protection to that afforded to the press (see Társaság a Szabadságjogokért[v. Hungary, no. 37374/05, 14 April 2009], § 27, and Animal Defenders International v. the United Kingdom [GC], no. 48876/08, § 103, 22 April 2013) – EctHR 28.11.2013, Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes v. Austria, 39534/07 § 34. Also see 17.2.2015, Guseva v. Bulgaria, 6987/07 § 38 and EGMR 27.5.2004, Vides Aizsardzības Klubs c. Lettonie, 57829/00 § 42.

19 Whereas it used to be widespread in 19th century England or the US at that time, for example – see Jason A. Martin and Anthony L. Fargo, Anonymity as Legal Right: Where and Why it Matters, 16 North Carolina Journal of Law and Technology 2015, 311 (322-327).

sisting the press in informing the public on matters of public interest[and] the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected."[20]

In particular, the Court pointed out in its later case law, regarding "the potentially chilling effect an order of source disclosure has on the exercise of [press] freedom, such a measure cannot be compatible with […] the Convention unless it is justified by an overriding requirement in the public interest;[21] a demanding balancing exercise, resembling the test Byron White developed in the famed, even if oftentimes criticized, majority opinion in the US Supreme Court case Branzburg v. Hayes Judgment,[22] as well as countless other efforts of national High Courts from Canada[23] to Japan[24] to ensure source protection, even if on a case by case basis. To adequately pursue this matter, however, would require a separate paper on this topic.

4. At the Core of a Free Speech Principle

In any case it seems sufficiently established that anonymity, from more than one perspective, rests at the very core of a free-speech principle according to the case of law referred to. And it impressively does so as well on the universal level which is amply demonstrated by the fact that when the International Covenant on Civil and Political Rights was negotiated, an

20 ECtHR (GC) 27.3.1996, Goodwin v. UK, 17488/90 § 39.

21 ECtHR 22.11.2012, Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, 39315/06 § 127. Also see, in particular ECtHR (GC) 14.9.2010, Sanoma Uitgevers B.V. v. the Netherlands, 38224/03 and ECtHR 15.12.2009, Financial Times Ltd and Others v. the United Kingdom, 821/03. But see ECtHR (dec) 27.5.2014, Sticting Ostade Blade 8406/06. For the Court's case law on searches and seizures intended to identify a source most recently ECtHR 19.1.2016 Görmüş and Others v. Turkey, 49085/07.

22 Branzburg v. Hayes, 408 U.S. 665 (700): "State's interest must be 'compelling' or 'paramount' to justify even an indirect burden on First Amendment rights." For a recent analysis of the consequences of the developments caused by Branzburg cf. Martin & Fargo (n. 21) 334-339.

23 See for the case law of the Supreme Court of Canada Moysa v.Alberta (Labour Relations Board), [1989] 1 S.C.R. 1572 and R. v. National Post, [2010] 1 SCR 477.

24 Supreme Court of Japan, 2006 (Kyo) 19, Minshu Vol. 60, No. 8.

amendment proposed by Brazil[25] to include the phrase "anonymity is not permitted" in its Article 19, was rejected emphatically.[26] Remarkably, it is this ubiquity that, upon closer examination, exposes the rationale for protecting anonymous speech as developed so far to be deficient: Of course, anonymous speech is elementary to a democratic society, precisely because it facilitates the creation of a public communicative sphere of common experiences; precisely because it enables and shapes public discourse; precisely because it is of such vital importance to public interest.

Still, that is not all: The right to speak freely and anonymously *may* serve a political function. It doesn't have to. Just as anonymous speech *may* have political content *and* be protected while it does not necessarily need political content in order *to* be protected. We may choose to speak anonymously on a large variety of topics and for a large variety of reasons.

John Mullan, for example in his survey of Anonymity in English literature distinguishes mischief, modesty, women being men, men being women, danger, reviewing, mockery, devilry and confession.[27] John Paul Stevens on behalf of a Supreme Court majority put it this way: "[T]he decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible;"[28] indicating in any case that, the equation: anonymous speech = political or social activism suffers from a lack of complexity.

Thus, if we want to assess the deeper significance of anonymous speech in a broader, and therefore more adequate perspective, we need to reflect generally on what anonymity allows us to do in conceptualizing ourselves within the framework of society.

25 See, Art 5 § IV of the Constitution of Brazil: 'manifestation of thought is free, but anonymity is forbidden.'

26 Marc J, Bossuyt, Guide to the "travaux Préparatoires" of the International Covenant on Civil and Political Rights (1987) 379-380.

27 John Mullan, Anonymity: A Secret History of English Literature (2007).

28 McIntyre v. Ohio Elections Comm'n 514 U.S. 334 (1995) 341-342. Also *see* Watchtower Bible & Tract Soc. of N. Y., Inc. v. Village of Stratton 536 U.S. 150 (2002).

5. Privacy in Speaking?

In doing that, we may find Stevens's last remark somewhat disturbing: Of course, we may readily assume anonymity at the core of a fundamental rights claim to privacy. But may speaking anonymously really be about preserving "as much of one's privacy as possible"? At the very least it sounds counter-intuitive: After all anonymous speech for whatever reason, so far as we have discussed the phenomenon until now, does not seem to be about the speakers intent "to be let alone",[29] as Warren and Brandeis famously put it, or her claim to a sphere that does not allow for any intrusion. Quite the contrary: Even if ideally, the concept of speech presupposes a willing speaker[30] and (even if only potentially) somebody to speak to; as "[c]ommunication is a joint enterprise, and only that joint enterprise triggers the principle of free speech."[31]Speech, no matter if of the anonymous variety or not, means to convey a message to others;[32] and to speak therefore means to open up rather than to seclude, to interact rather than to stay put.

So is it really correct to talk about privacy in speaking?

It is; even if understanding this presumes to deviate from the narrow concept of privacy I just introduced and to focus on the purposive approach the Canadian Supreme Court among others had long applied on Art 8 of the Canadian Charter "that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfillment and autonomy as well as to the maintenance of a thriving democratic society".[33] The European Court of Human Rights introduced a similar thought in its Niemietz Judgment in

29 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Review 1890, 193 (205).

30 Virginia Pharmacy Board v Virginia Consumer Council, 425 U.S. 748 (1976) 756.

31 Frederick Schauer, Free Speech: a philosophical enquiry (Reprint 1984) 98.

32 Even if the message does not have to be „a narrow, succinctly articulable" one - Hurley et al v Irish-American Gay, Lesbian and Bisexual Group of Boston, Inc, et al, 515 U.S. 557 (1995) 569.

33 R. v. Spencer, [2014] 2 S.C.R. 212 § 15 referring to Hunter v. Southam Inc., [1984] 2 S.C.R. 145, 156-57, R. v. Dyment, [1988] 2 S.C.R. 417, 427-28, R. v. Plant, [1993] 3 S.C.R. 281, 292-93, R. v. Tessling, 2004 SCC 67, [2004] 3 S.C.R. 432, §§ 12-16 and Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, [2013] 3 S.C.R. 733 §22.

1992[34] and developed it further in its case law over the past years arguing that the protection of one's 'private life' is "not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. [...] There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'".[35]

If we thus perceive the protection of private life to encompass an individual's self-determined development in interaction with others,[36] we may readily conclude that a fundamental rights claim to privacy and a fundamental right to free expression are deeply interwoven; creating a safe sphere of sovereign decision which aspects of one's personality to disclose, what to communicate, whom to speak to, whom to avoid.[37]

A right to self-determined social interaction so composed grants broad discretion to the individual in answering those questions; holistically safeguarding a person's prerogative in deciding what to realize and how to realize oneself in society.[38]

It is therefore indeed, as the previous Special Rapporteur on Freedom of Expression for the Inter-American Commission on Human Rights recently held, "*[b]oth* the right to freedom of thought and expression and

34 ECtHR (GC) 16.12.1992, Niemietz v. Germany, 13710/88 § 29.

35 ECtHR 21.6.2011, Shimovolos v. Russia, 30194/09 § 64. See, for the Court's more recent case law ECtHR (GC), 12.6.2014, Fernández Martínez v. Spain, 56030/07 § 126 and ECtHR 12.1.2016, Bărbulescu v. Romania, 61496/08 § 35.

36 See in comparative perspective Avner Levin & Mary Jo Nicholson, Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground, 2 University of Ottawa Law & Technology Journal 2005, 357 and Michael C. James, A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe 29, Connecticut Journal of International Law 2014, 257.

37 For a recent discussion of this topic see i.a. Bart van der Sloot, Privacy as Human Flurishing, 5 JIPITEC 2014, 230 and R.L. David Hughes, Two Concepts of Privacy, 31 Computer & Security Law Review 2015, 527.

38 The "Right to be Forgotten" (ECJ [GC] 13.5.2014, Google Spain SL) is the most recent example for this perception –see, i.a., Richard Spinello, The Right to Privacy in the Age of Digital Technology, in Zeadally & Badra (eds), Privacy in a Digital, Networked World (2015) 291.

the right to private life that protect anonymous speech from government restrictions;"[39] and perhaps even closer to my understanding, as Lord Neuberger put it: "In the context of anonymous speech, an author's [privacy] rights reinforce his or her [free speech] rights".[40]

It is a related, yet divergent rationale that shields encrypted communication from undue government interference. I would like to make that point rather quick. But still, even if the academic and professional discourse on the topic oftentimes mixes anonymity and encryption together as they both are concerned with disguised communication, it is important to point at an essential difference: while anonymity disguises the messenger, encryption disguises the message. And therefore the picture of the anonymous pamphleteer, addressing public grievances, is ill-fitted as a starting point of examining encryption in the first place; because – if this simplifies rather complex issues: The pamphlet craves the light of the public, the encrypted message shuns it.

The consequences of this observation are, of course, of some importance as far as the angle from which to address it in a fundamental rights perspective is concerned: Encrypted communication primarily seems to have a fundamental rights claim based on privacy considerations like the protection of "correspondence" as article 17 of the ICCPR and – following its wording – 8 ECHR put it, or the protection of "communication" in the sense of article 7 of the EU Charter of Fundamental Rights. Encryption provides security so that individuals are able "to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion",[41] as encryption is of invaluable importance when it comes to communication of sensitive topics like illness, religion or sexual orientation.[42]

39 Catalina Botero Marino, Freedom of Expression and the Internet (2013) § 134 (my emphasis).

40 Lord Neuberger, "What's in a Name?" – Privacy and anonymous speech on the Internet, Keynote Speech Conference5RB, 30.9.2014 § 25.

41 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 22.5.2015, A/HRC/29/32 § 17.

42 See e.g. Stephen Stratton, Janet Dean, Mark Yarhouse and Michael Lastoria, Sexual Minorities in Faith-Based

And yet one must not underestimate the great extent to which claims deriving from a right to privacy and such claims deriving from a right to free speech are interrelated as far as encrypted communication is concerned; being of essential importance, not only as far as the freedom to hold opinions but also as far as the freedom to seek, receive, and impart information and ideas is concerned:[43] It would be wrong to simply sum up the phenomenon by stating that anonymous sources want to talk while encrypted sources intend to remain silent: Far too often encrypted communication turns out to be the necessary prerequisite for subsequently bringing to light that kind of information which could only be transmitted far from the public eye.

In any case, for now, it may be sufficient to reverse Lord Neuberger's remark on anonymous speech as far as encrypted messages are concerned: "In the context of encrypted speech, an author's [free speech] rights reinforce his or her [privacy] rights".[44]

Of course, this twist has no immediate impact on the result regarding both of the fundamental rights claims in question: As Frank La Rue, then Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated in his 2013 Report to the Human Rights Council, assessing the problems before us: "Privacy and freedom of expression are interlinked and mutually dependent".[45] Consistently we may agree with the conclusions his successor David Kaye reached in his 2015 report: that encrypted and anonymous messages indeed enjoy the protec-

Higher Education: A National Survey of Attitudes, Milestones, Identity, and Religiosity, 41 Journal of Psychology and Theology 2013, 3. For select (approaches to the) problems in the various fields see i.a. Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi & Pierangela Samarati, Fragmentation and Encryption to Enforce Privacy in Data Storage 171, in Biskup & Lopez (eds), ESORICS (2007) 171, Yitzchak M. Binik, Kenneth Mah & Sara Kiesler, Ethical Issues in Conducting Sex Research on the Internet, 36 The Journal of Sex Research 2010, 82, Rajeev Kumar, Ram Gopal, Robert Garfinkel, Freedom of Privacy: Anonymous Data Collection with Respondent-Defined Privacy Protection, 22 INFORMS Journal on Computing 2010, 471.

43 Frank LaRue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 17.4.2013, A/HRC/23/40 §§ 24-27.

44 Neuberger (n. 39) § 25.

45 LaRue (n. 42) § 79.

tion of the rights to privacy and freedom of expression.[46]

6. Modes of Communication

To leave it with this observation, however, would prove to be somewhat unsatisfactory, or so I assume. Because it keeps ignoring the elephant in the room: What does it mean that fundamental rights claims to privacy and freedom of expression *enjoy* a right to anonymous or encrypted communication? Of course, I will not be able to give you one, or even a coherent, answer to that question. Please do allow me, however, the following general remarks. In order to do this, let us take one step back, highlighting two points of Kaye's report:

First by a remark as to the way anonymity and encryption are related to a general concept of speech protection. Kaye's report relies on describing encryption and anonymity as specific *media* through which individuals exercise their freedom of expression[47] (reinforced, or backed up by their right to privacy, I would like to add). He does so, evidently, against the backdrop of case law shaped in particular by the European Court of Human Rights whereas "Article 10 ECHR protects not only the substance of the ideas and information expressed but also the form in which they are conveyed."[48] Which is why "all means of expression are included in the ambit of Article 10 of the Convention."[49]

True enough. But are encryption and anonymity indeed means of communication in that sense? Or to come back to the point Kaye made in his report: Are they *media*, employed in order to serve as a carrier of a message to be conveyed? You realize by the way I phrase the question that I am not keen to answer it affirmatively: To communicate anonymously or in an

46 Kaye (n. 40) §§ 14-28.

47 Id. § 26.

48 *See*, i.a., ECtHR 23.5.1991, Oberschlick v Austria (No 1), 11662/85 § 57; (GK) 24.9.1994, Jersild v Denmark, 15890/89 § 31; 24.2.1997, De Haes and Gijsels v Belgium, 19983/92 § 48; 29.3.2001, Thoma v Luxembourg, 38432/97 § 45, 12.9.2011, Palomo Sánchez v Spain, 28.955/06 ua § 53 and for the Court's more recent case law 28.10.2014, Gough v UK, 49327/11 Rn 149.

49 *See*, for the Court's recent case law ECtHR 21.10.2014, Murat Vural v Turkey, 9540/07 § 52.

encrypted manner does not constitute a medium; it rather presupposes it. And thus it says not that much about the medium employed; as little in fact as it tells us about the content that is communicated.

Much more than to constitute a specific medium, to communicate anonymously or in an enycrypted manner means to make use of a certain *mode* of communication. A mode that may apply to a large variety of different media as well as it may be applied to communicate a large variety of different messages. Anonymous or encrypted communication thus may well be regarded as a layer to be spread across the body of fundamental rights doctrine to be applied, allowing for a specific emphasis on those issues where these modes of communication may have particular use.

Now to approach the second point: Kaye's Report, as well as the conclusion he draws, is primarily concerned with anonymity and encryption in digital communication and thus, of course, with the most important field of application for the topic I'm addressing. Indeed, it is evident, that today, when we are discussing anonymity and encryption, letters to the editor of a newspaper are no longer at the very center of our attention. Save for Dan Brown Novels, the same applies to coded messages handed from one person to another. Nowadays at the very center of our attention we find the global network that so significantly altered our means of communication and continues significantly to shape public discourse as well as the political landscape.

Indeed: "The Internet has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it."[50] Its "transformative nature […] giv[es] voice to billions of people around the world".[51] And, as Lord Neuberger emphasized, the Internet "offers unprecedented opportunities for such self-development."[52]

50 Kaye (n. 40) § 11.

51 The United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet, 23.5.2011.

52 Neuberger (n. 39) § 14.

This has, of course, long since been recognized in free speech case law: John Paul Stevens, writing for a Supreme Court majority, emphasized already back in 1997 that "[t]hrough the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer."[53]

It is this amplifying function that, as the ECtHR emphasizes on a regular basis,[54] makes tools available on the internet powerful as well as dangerous. And even more so if employed anonymously. And – even though from a different perspective – the same may apply to conveying encrypted information which – in an advanced manner previously only at the disposal of governments – is drastically facilitated by modern technological means readily available.

As Kaye concludes: "Terrorists and criminals may use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity […] cowardly mask[ing] discrimination, particularly against members of vulnerable groups."[55]

In particular as far as the latter problem is concerned, psychologists have noted that publicly communicating anonymously may indeed have a significant disinhibited effect on the communicator who then is liberated from the ties of open interaction according to the general social framework.[56] This, of course, hardly comes as a surprise. More than two Centuries ago Benjamin Franklin observed that anonymity: "enabled men of

53 Reno v. American Civil Liberties Union 521 U.S. 844 (1997) 870.

54 See, i.a. ECtHR 22.4.2010, Fatullayev/Azerbaijan, 40984/07 § 95, 18.12.2012, Yıldırım v. Turkey 3111/10 § 48 and, in particular, (GC) 16.6.2015, Delfi AS v. Estonia, 64569/09 § 110..

55 Kaye (n. 40) § 13.

56 See, in particular, John Suler, The Online Disinhibition Effect, 7 CyberPsychology & Behavior 2004, 321. For a more recent study see Noam Lapidot-Lefler & Azy Barak, Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition, 28 Computers in Human Behavior 2012, 434.

honor to behave dishonorably".[57] And yet there is more to it, if we decide to give it a closer look, as *honor* or to put it in more modern terms: *reputation*, so painstakingly built and so carefully guarded in our social interactions off-line cannot serve its diverse functions in a sphere that allows the individual to dissolve the ties of recognition and accountability: "Anonymity and fluidity in the virtual world", Robert Putnam observes, "encourage 'easy in, easy out,' 'drive-by' relationships. The […] casualness […] of computer-mediated communication […] discourages the creation of social capital. If entry and exit are too easy, commitment, trustworthiness, and reciprocity will not develop."[58]

Thus, rather than to just disown a reputation, previously built, "anonymity inhibits the process by which reputations are formed"[59] in the first place. The global village – assessed from this perspective – starts to resemble the "great city", Adam Smith describes in "The Wealth of Nations", where the common man is "sunk in obscurity and darkness[; where h]is conduct is observed and attended to by nobody, and he's therefore very likely to neglect it himself, and to abandon himself to every sort of low profligacy and vice."[60]

True enough: The shield of anonymity obviously tends not always to bring out the very best in us. Or to put it more bluntly, vindicating my history teacher: indeed, the shield of anonymity obviously tends to bring out the scoundrel from time to time; and secrecy by way of encryption, it may be added in the given context, may well abet him.[61] And we have to consider all these specific problems, when spreading our layer of fundamental rights doctrine over cases where the *modes* of anonymous or encrypted communication meet the amplifying function of digital tools.

57 Shalev (n. 11) 158.

58 Robert Putnam, Bowling Alone: The Collapse and Revival of American Community (2000) 177.

59 Daniel J. Solove, The Future of Reputation (2007) 141-142.

60 Adam Smith, An Inquiry Into the Nature and Causes of the Wealth of Nations [1776] (Cannan ed.), vol. 2 (1904) 280.

61 Just see Paul Bocij & Leroy McFarlane, Cyberstalking: The Technology of Hate, 76 The Police Journal 2003, 204 (210-211).

7. The Length of the Leash

Sure enough: How these problems are dealt with, evidently depends on the specific legal system we are talking about and the fundamental rights standards to be applied in these systems. Vietnam, for example, outlawed the use of pseudonyms in 2013; forcing bloggers to reveal their identity.[62] Iran requires all IP addresses used for blogs in the country to be registered.[63] Russia obliges popular bloggers the register with the national media regulator[64] and China, most prominently, introduced a real-name registration requirement several years ago,[65] which according to government announcements dating from last year is to be strictly enforced.[66]

The Korean Constitutional Court in a judgment of 2012 on the other hand struck down a statute requiring general online real name verification: As a [rule that] mandates identity verification regardless of the content of [a] posting from almost all users on all major websites [would cause a significant chilling effect, the court argued].[…]. Such [a] result of suppressing a great majority's legal postings on the account of the existence of a minority of people abusing the internet[, the Court went on to argue,] is an excessive restriction on freedom of anonymous speech …. [i]t treats all people as potential criminals in favour of investigative expediency.[67]

This reason, it seems to me, may, in a nutshell, well serve as a description of the fundamental rights standard to be applied according to the diverse considerations outlined before: Anonymous and encrypted speech on the internet, though fraught with harmful side effects, should be strongly protected in view of its fundamental rights value. Strongly, although not absolutely: as these harmful side effects need to be addressed and eventually

62 See Martin and Fargo (n. 21) 362.

63 See, i.a., Saeid Golkar, Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran, 9 International Journal of emerging Technologies and Society 2011 50 (60).

64 See, i.a. Andrey Tselikov, The Tightening Web of Russian Internet Regulation, Berkman Center Research Publication No. 2014-15.

65 See Jyh-An Lee & Ching-Yi Liu, Real Name Registration Rules and the Fading Digital Anonymity in China, 25 Washington International Law Journal 2016, 1.

66 WSJ 4.2.2015, China Is Requiring People to Register Real Name for Some Internet Services.

67 KCC 23.8.2012, 2010Hun-Ma47.

regulated; oftentimes just to effectively safeguard fundamental rights of individuals negatively affected by the actual or potential actions of others as well as to ensure public safety and well-being.

And so, even if the result of the Delfi judgement, delivered by the Grand Chamber of the European Court of Human Rights last year,[68] may well be criticized;[69] the general rationale underlying it, albeit originally developed in an earlier judgment, seems perfectly reasonable: "[A]lthough freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."[70]

To transpose this into commonly accepted fundamental rights terminology: Anonymity and encryption may be restricted by law in order to pursue certain legitimate aims applying a strict proportionality standard. As even encryption and anonymity on the Internet, "although […] important value[s], must be balanced against other rights and interests".[71] Following the arguments introduced by the Supreme Court of South Korea, indiscriminate requirements like ubiquitous real-name registration requirements or general bans on encryption, however, will hardly pass effective fundamental rights scrutiny along these lines.

Still, we see that just because the fundamental rights to privacy, freedom of press and freedom of expression do entail a right to anonymous or encrypted communication, that does not mean that the scoundrel is unleashed… What we will have to keep discussing, however, is how long the leash ought to be: Because the answers to the questions whether or not to grant governments back-door access to encrypted data as is currently passionately discussed in the US,[72] whether or not to accept prior approv-

68 Delfi v. Estonia (n. 53).

69 See, i.a. Martin Husovec, General monitoring of third-party content: compatible with freedom of expression?, 11 Journal of Intellectual Property Law & Practice 2016, 17.

70 Delfi v. Estonia (n. 52) § 149 referring to ECtHR 2.12.2008, K.U. v. Finland, 2872/02 § 49.

71 Delfi v. Estonia (n. 53) § 149.

72 See, i.a., Reema Shah, Law Enforcement and Data Privacy: A Forward-Looking Ap-

al for the use of VPNs as in Pakistan[73] or the ban of certain encryption standards as in India,[74] whether or not to justify warrantless acquisition of anonymous online identities as recently quashed by the Supreme Court of Canada[75] and under which circumstances to hold intermediaries accountable for third-party statements as debated within the European system of human rights protection at present,[76] will decide the fate of our capacity for self-determined social interaction beyond the ever present scrutiny of our environment.

proach, 125 Yale Law Journal 2015, 542.

73 See, i.a. Zubair Nabi, The Anatomy of Web Censorship in Pakistan, arXiv:1307.1144 [cs.CY].

74 See, i.a., A. Parvathy; Vrijendra Singh, Ravi Shankar Choudhary, Legal Issues Involving Cryptography in India, 8 Vidhigya 2013, 1.

75 R v. Spencer [2014] 2 SCR 212.

76 See, i.a., Lisl Brunner, The Liability of an Online Intermediary for Third Party Content – The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia, 16 European Human Rights Law Review 2016, 163. For the ECtHR's case law see, most recently, ECtHR 2.2.2016, Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, 22947/13.

b. Specific issues

The State vs Oscar Pistorius: A Critical Analysis of the Court of Public Opinion

by Abraham Gert van der Vyver[1]

1. Introduction

The Oscar Pistorius case in which this paralympic megastar was prosecuted for the shooting of his girlfriend, Reeva Steenkamp, grabbed the imagination of millions throughout the world. The case generated a tsunami of public responses thereby clearly indicating the growing importance of the social media. Social media like Facebook and Twitter were turned into a court of public opinion. Citizen journalists competed vehemently against professional journalists for scoops and novel news angles. With the case being televised in real time, the playing field was now level.

In this paper, a concise analysis of the extant literature pertaining to relevant constructs like public sphere, public opinion, citizen journalism, professional journalism and the social media will be discussed. The methodology used for sampling, data collection, and analysis will be described. Subsequently the findings as well as suggestions for future research, will be addressed.

2. Literature review

2.1 The public sphere

Over the past decade scholars and commentators have enthusiastically applauded the rise of citizen journalism. It has been seen as the advent of a

1 Abraham Gert van der Vyver is a senior lecturer at School of IT, Monash, South Africa. He has obtained degrees in law, marketing, communication, and information systems and the other authors may include biographies at the end of regular papers. His PhD is in political communications. He has also obtained an Australian Higher Education Diploma. His fields of interest and research are social informatics, development informatics, cyberlaw, and ethics.

true public sphere, a concept that grabbed the imagination for centuries.

The public sphere of the 18th century was described as elitist and bourgeoisie. According to Hauser [1] it is a discursive place where people can interchange their opinions to create a common judgment. According to Habermas [2] "the bourgeois public sphere flourished in the high-minded and open London coffeehouses and Parisian salons of the eighteenth century." Habermas warned that "(t)his critical nature is endangered by the power of the mass media that transforms most of the society in a passive public, the objectives of a consumer's culture" [1]. The task of a public sphere is that society can become engaged in "critical public debate" [2]. The public sphere would therefore require media for information and communication and access by all citizens. The social media of today is probably the closest one can get to the idealistic phenomenon that Habermas described. Goldberg [3] acknowledges that there is an array of viewpoints on what constitutes the modern public sphere. "I will assume a basic and widely shared definition: a site of social activity comprised of rational discourse which occasions the informal constitution of the public will."

2.1.1 Public opinion

It is ironic that a high profile court case like *The State v. Oscar Pretorius* triggered a total rethink of the Court of Public Opinion, a concept that has been debated in the P.R. domain for decades. The case of O.J. Simpson needs no introduction. The retired football star and actor was acquitted of killing Nicole, 35, his ex-wife, and her friend Ronald L. Goldman, in her Los Angeles home. The popular publication, Macleans, reported before the trail that "But already the case is being tried in the court of public opinion. Leaks to the media by anonymous police sources have created a circus-like atmosphere. Among damaging reports that were debunked last week was one that police had found a blood-stained ski mask at the crime scene" [4]. According to Hudson, "(i)t's hard not to notice the rapidly increasing volatility in the relationship among the law, the press and public relations. The three professions' objectives often intersect, frequently coincide and more frequently collide" [5].

Bady [6] feels that there is no such thing as the Court of Public Opinion.

> When people use the phrase, they strongly imply—even outright

> state—that newspaper articles, op-eds, "litigation by hashtag," and general opinion-having by the unwashed masses constitutes a kind of parallel legal system in which "mob justice" is meted out by "villagers with torches." In the Court of Public Opinion, they believe, "the one-eyed man with the most Twitter followers is king," and all the checks and balances of law and order are suspended

Scheier [7] differs from him and declares Facebook and Twitter as battlegrounds where these reputational battles are fought.

> "The court of public opinion is an alternative system of justice. It's very different from the traditional court system: This court is based on reputation, revenge, public shaming, and the whims of the crowd. Having a good story is more important than having the law on your side. Being a sympathetic underdog is more important than being fair."

Pistorius implemented an unconventional strategy by employing a team of public relations experts to manage his presence in the public domain. The International Business Times revealed that "Just days before his murder trial begins, Oscar Pistorius' PR team have created a Twitter account which they say will reveal the "hard truth" surrounding the court proceedings" [8].

According to the British daily newspaper, The Independent, Pistorius employed the services of a London-based PR practitioner, Stuart Higgins who immediately showed his hand. "Mr Pistorius's PR team were relaunching the athlete's website to publish sympathetic comments he has received. "Our job is to capture some of the support that Oscar is receiving from all over the world, lots of positive messages from people who still believe in him," said Higgins [9].

Part of the Twitter war that erupted during the Pistorius-case was fought between followers and adversaries of the disgraced athlete.

2.1.2 Professional journalism vs. citizen journalism

A professional journalist is, for the purpose of this study, an individual who earns an income from producing content from a media outlet. All professional journalism, whether analog or digital, has at its core an aspiration toward accuracy, precision in communication and fairness [10]. In order

to subscribe to these values, most professional journalists belong to professional associations. These so-called press clubs promote and enforce their own ethical codes. The Oscar Pistorius trial has been commemorated as the National Press Club's Newsmaker of the Year for 2014. "This includes the roles played in the trial by Oscar Pistorius himself, Judge Thokozile Masipa, prosecutor Adv Gerrie Nel and defense lawyer Adv Barry Roux." [11].

The question immediately arises whether this statement also applies to the world of journalism where thousands of citizen journalists are in competition with professional journalists.

Citizen journalism that is defined as "the process of members within the public playing an independent role in collecting, reporting and distributing, current and breaking news events, has recently become very popular" [12].

"Citizen journalism is defined by a number of attributes which make it distinct from professional journalism, including unpaid work, absence of professional training, and often unedited publication of content, and may feature plain language, distinct story selection and news judgment, especially hyper-local issues, free accessibility, and interactivity"[10].

According to Harper [10], "the increasing presence, speed and accessibility of advanced cellular phones and other media sharing devices has allowed citizen journalists to report on breaking news not only to a larger, global, audience, but also more quickly than traditional news reporters." After the September 11 attacks, Gillmor [13] wrote:

> But something else, something profound, was happening this time around: news was being produced by regular people who had something to say and show, and not solely by the 'official' news organizations that had traditionally decided how the first draft of history would look. This time, the first draft of history was being written, in part, by the former audience. It was possible–it was inevitable–because of new publishing tools available on the internet.

The advent of the social media not only provided an array of new and highly accessible platforms for citizen journalists to apply their trade, it also underscored the dualism between professional journalism and citizen journalism. Both forms of journalism are conducted according to their own set of rules and governed by their own gatekeepers yet they all fall within the

broad domain of journalism.

Citizen journalism that is defined as "the process of members within the public playing an independent role in collecting, reporting and distributing, current and breaking news events, has recently become very popular [3]. Citizen journalists often get the news in the public domain before the professional journalists because they are less hampered by the codes and conventions of the news room. The only gatekeepers they face are the editors of the electronic platforms on which they publish. Harper [10] pointed out that "(n)ew media technology such as social networking eg: Twitter, Facebook and Blogger, have given everyday citizens the ability to transmit information globally; a power which was once only reserved for large media corporations."

Where professional journalism is a fully-fledged profession regulated by codes and conventions that are enforced by professional bodies, most citizen journalists function as free agents. Gatekeeping is the process that distinguishes these two practices. Harper explained:

This relies on all experienced and trained journalists and editors to filter any nonfactual information from news reports before publication or broadcasting. Citizen journalists are untrained in such journalistic methods and are therefore at risk of using unreliable sources and publishing incorrect or in-factual news [3].

Gatekeeping also applies to participatory journalism. Participatory journalism that originated as the letter columns in the printed media has now evolved to multimedia platforms provided by established media. CNN launched its iReport website on 2 August 2006. iReporters draw on CNN's clout to disseminate their messages across a wide variety of multimedia platforms. Their unpaid labor simultaneously bolsters the power of the CNN brand while also illuminating the social hierarchies long associated with traditional journalism, thus serving as an example of the increasingly "symbiotic relationship" between mainstream media and citizen journalists [14].

In the case of iReport the producer of the webpage verifies the content. The contributor is contacted if necessary [15].

Goode [16] pointed at two other dimensions of the definition of citizen journalism that needs to be taken into account. Firstly, citizen journalism is not restricted to digital content. Broadcast news often include eyewitness

footage from cell phones while print media incorporate soapbox features [16].

Secondly, Goode [16] raised what he called "the most vexing question about the boundaries of citizen journalism" namely "whether we should restrict its definition to practices in which citizens act as content creators, producing original news material." This question relates to other ways citizens voice an opinion or make a contribution to the news environment e.g. by "rating, commenting, tagging and reposting," all acts of contribution that is seen as "considerably less significant than 'real' citizen journalism" [16]. Goode offered the following clarification: "if a user posts a comment on an existing news story but, in doing so, brings to light new knowledge about that event or topic, then it is not clear that this contribution can be classified only as 'metajournalism'. Features such as hashtags and retweeting help spread news and information faster than other media, whether in normal or crisis situations, and get people with shared interests closer to each other [17]. As such, a broad conception of citizen journalism appears warranted on the proviso that the important democratic function of bringing new knowledge into the public sphere is not downgraded as equivalent to secondary commentary" [16].

In the Twitter analysis that forms the empirical part of this paper, tweets represent both broad categories, i.e. new information and/or opinions but also the mere recycling of other people's contributions. Some of the tweets in the sample have been the subjects of large-scale metajournalism.

2.1.3 The social media

During the last decade the social media has become the dominant force in cyberspace. Alejandro [18] explained that "the great wave of web innovation since Google in 1998 has been in social media. Social media is about networking and communicating through text, video, blogs, pictures, status updates on sites such as Facebook, MySpace, LinkedIn or microblogs such as Twitter."

More and more readers, listeners and viewers are going online to get their news. Newspapers and magazines that determined the news agenda for many decades have closed down or gone online. "What makes social media of particular interest to journalism is how it has become influential as a communication and news-breaking tool" [18].

There can be no doubt that the conventional media faces severe compe-

tition from citizen journalists. Krotoski writing in the The Guardian (UK) acknowledges that the conventional media has lost the battle [19].

> "(T)echnology has improved the processes of identifying stories that are newsworthy. Feeds from social networking services such as Facebook and Twitter provide a snapshot of events happening around the world from the viewpoint of first-hand witnesses, and blogs and citizen news sources offer analytical perspectives from the ground faster than print or television can provide."

The Oscar Pistorius case has caused such a media rush that competition between the conventional media and the social media reached ballistic levels.

In this paper, the role of Twitter as a tool for professional journalists as well as citizen journalists is investigated. Twitter is an online social networking and micro-blogging service, which allows users to write short messages or tweets as text and to send these to the system. There is a limit of 140 characters per tweet. Users are also able to follow other users of Twitter and view their tweets. Unregistered users are only able to read tweets posted, but are not able to respond to a tweet or to quote (re-tweet) the message [17]. "Tagging enables you to link a picture, post, or status to another user or business. Tagging not only alerts users that they have been tagged in something relevant but it also increases the reach of the post or tweet" [20].

2.1.4 The ethics of journalism and social informatics

The dualism between professional journalism and citizen journalism has forcefully impacted on the ethical domain. «We stand at a moment when the journalistic ethical codes that American society has known for decades are now are under tremendous pressure, as the underlying business model continues to erode, news and information are increasingly consumed in personalized ways on commercial platforms, and every journalistic story must compete for attention amid an overwhelming sea of what is generically being called "content"» [12].

It is clear that the playing field for professional journalists and their citizen peers is not level. No logical solution is on the cards. The legendary Walter Lippman, American journalist and political commentator was not convinced that journalists were good at providing their readers and/or audiences with the truth [21].

The most journalists do, Lippman argued was to "signalize an "event" in one spot for a moment, leaving the area around it in darkness. That signalizing is like a spotlight that focuses on new facts while the context of these facts, "the picture of reality on which men can act" remains hidden in the shadows. That's news, not truth [22].

3. Research methodology

The author analysed tweets from professional journalists as well as tweets from citizen journalists. Purposive sampling of tweets was conducted during a ten day window during the trail." These tweets were then divided into two categories, namely tweets from professional journalists and tweets from citizen journalists. Where relevant, comparisons were drawn. The American Association for Public Opinion Research is of the opinion that "(t)here are legitimate quality concerns with using social media in research. Not every member of the public uses these platforms and those who do use them in different ways. In this respect, social media may provide useful insights for a particular set of questions, but perhaps not more specific point-estimates which are generalizable to a broader population." In this case the author conducted an interpretive analysis. No quantification was executed.

3.1 Twitter analysis

3.1.1 Tweets by professional journalists

The second tweet in the sample contained a strong historical reference. It reads: Scorched earth policy by Nel as he goes through some amended dates for photo trying to leave #OscarPistorius defense nothing to challenge. It was posted by a BBC reporter which explains the reference to the British war practice of destroying anything that may be useful to the enemy. The principle was applied to the tactics used by the public prosecutor who handled the case against Pretorius. The tweet proves that the journalist thought laterally and creatively about the case and that he has a knowledge of war history.

Media can use tweets to focus the attention on other multi-media initiatives they have staged In the tenth tweet in the sample, City Press, a leading Sunday newspaper tweeted a reference from Deborah Patta, an influential investigative journalist who conducts video reports on its behalf. This il-

lustrates the major paradigm shift that many conventional newspapers embarked upon in the environment. The tweet reads; "@Debora_Patta's diary: When can you shoot an intruder?"

A news monitoring service, News Detector, retweeted the following tweet from news24: Oscar Pistorius trial enters pop culture http://n24.cm/1iSb7Ho. The original tweet refers to an article that appeared on the website news24. The article gives examples of how the case has grabbed the imagination of the general public and how it impacted on group and individual behaviour. The journalist who was not named wrote "Turns of phrase from the courtroom - the defense lawyer's "I put it to you" challenge to prosecution witnesses - are creeping into popular culture".

A tweet from 567Cape Talk reads OscarPistorius accepts a gift from a supporter while leaving court after his 5th day in the witness box. http://bit.ly/1erDEC2. The link opens to an Instagram photo where Pretorius accepts the gift as well as an update from Eye Witness News that reads:

ewnupdates As #OscarPistorius left the High Court in Pretoria, a supporter was waiting outside with flowers and a book of prayer for the athlete. She says he needs to know he has her support.#OscarTrial

The tweet "31 seconds of silence: http://ow.ly/vJfiU" serves as a cross-reference to a news report in City Press that was also published on the4 news24 website. The introductory paragraph of the report reads:

"Thirty-one seconds – that's how long Oscar Pistorius was silent for when asked by Prosecutor Gerrie Nel if he heard Reeva Steenkamp scream after he fired the first of four shots that killed her."

The tweet is an example of a tweet that could not have been created by an individual who was not present in court since Pretorius's evidence was not televised.

Another tweet that cross-referenced an article in a popular electronic newspaper, The Daily Maverick, reads: Oscar's 'involuntary action': Thin ice, Mr Pistorius http://tinyurl.com/o8be47o by PIERRE DE VOS .@pierre-devos.

De Vos, a law professor at the University of Town, is highly critical of Pretorius's explanation of his state of mind during the shooting. The article is based on expert opinion. De Vos extensively referenced another case, S. v. Humphreys, in which the same legal questions were asked. Regarding the Pistorius case, De Vos explained:

[U]nder cross-examination Pistorius seemed to suggest that the gun had gone off in his hands, but that he had nothing to do with it. This defence – if it was indeed the defence offered by Pistorius – is not easy to sustain. However, if it is sustained, the accused is acquitted of all charges. This is so because it is a trite principle of our law that a voluntary act is an essential element of criminal responsibility.[6]

It needs to be pointed out that expert opinion can also be leveled in the form of citizen journalism with reference to a blog or a vlog.

The next tweet was posted by the esteemed journalist, David O' Sullivan on behalf of EWN. It reads "Coverage of Oscar trial reached highest point yet, according to Tonya Khoury from @DDIAfrica: pic.twitter.com/Rr1FqFa3tZ" and refers to a graph of the media coverage patterns released by, DDIAfrica, a well-known media research concern.

Journalists also linked to other genres as the following example of a cartoon illustrates. The tweet read "Masipa: OP knew that there was a person behind the door, he chose to use a firearm - Guilty of Culpable Homicide - http://www.zapiro.com/Pistorius-Right-to-a-fair-trial-140227tt/…"

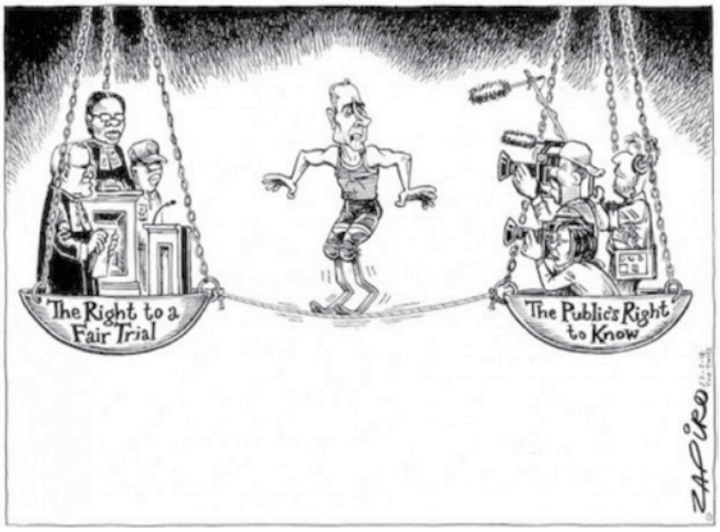


Figure. 1 Cartoon of Oscar Pistorius [24]

A video link was also referenced by AIO News. The tweet referred to a yelling noise made by a neighbor who imitated the sound she heard from the

crime scene. It read: "#OscarPistorius's neighbour imitates 'high pitched scream' - video http://q.gs/6tQr7"

3.1.2 Tweets by citizen journalists

Citizen journalists are not bound by ethical rules and gatekeeping practices. They do not hesitate to ask tough questions. In the first tweet in the sample the following question was posed:

If you fear for life with broken window on ground floor...why not activate alarm? #OscarTrial199 #oscarpistorius #oscartrial

A professional journalist would have to adopt a more subtle approach to address such an issue.

The problems with the interpreters that performed in the case were well-documented. One tweet stated in no uncertain terms that "We need an interpreter to interpret the interpreter" #OscarTrial #OscarPistorius. Another contributor was more direct: "This translator is embarrassing_kick her off and get someone who can translate clearly and properly".
The following two tweets were written in interrogation mode:

> "How on earth is there a blood splatter on the wall above the bed when the shooting was in the bathroom?" "Blood splatter above #OscarPistorius headboard? This is getting interesting. Did he assault her in the bedroom and she ran to the loo?"

Not only can citizen journalists get away with the use of informal terms like loo, they can also get away with abbreviations and acronyms that have a vulgar meaning as illustrated by the following tweet: "Firearm fetish, perhaps?? WTF" This tweet undoubtedly resembles a line from a stand-up comedy routine.

The rules of grammar and spelling do not apply to citizen journalists. They often sacrifice accurate spelling in order to retain the core message and there is no sub editor to veto the tweet. "Can someone pls explain the bloodied bat, blood splatter on/under duvet and left side of the bed".

Personal queries can be embedded in the writings of citizen journalists. The following tweet proves this point: "Am I really being too naïve by believing OP didn't do it on purpose?"

There is no embargo against sarcasm in citizen journalism. "Roux wanted to bring in the metadata yesterday. That says a lot about his knowledge of

cameras." Another tweet read: "you'd think the police would have learnt not to tamper with evidence at scenes. I mean even I know that from watching TV."

Twitter is often a playground for hostile and/or comic rants. "This young man #OscarPistorius will regret day he was born. At rate his defence claims (R50 000/day) he's gonna sell his artificial limbs too."

Twitter has no prescriptions regarding style and tone. The following tweet, despite poor syntax, displays suspicion: #OscarPistorius ... natures call & whilst he was being careful & quiet, surely Reeva would've flushed & OP would have heard the flush?"

"Oscarpistorius said towards end of Friday he "knelt down". HUGE, I hope #Gerrienel picked it up. He had his prosthesis on." An important anomaly is pointed out.

This microblog can also be used to introduce technical detail that was not mentioned in court: "U can't use2 dif camera's metadata re. time to compile the same sequence. they must be seperate as times can b set different."

Procedural matters can in Twitter be addressed in unconventional ways. "With all the adjournments it should be like football injury time and added on the end of the day, finishing at 3.30 is daft."

Many of the tweets carried strong opinions about the credibility of testimony."The only - but huge - inconsistency w #OscarPistorius' story so far: wounds suggesting Reeva was in a defensive position (& prob screaming)."

Similar content is allowed in reports of conventional journalists. A tweet like "Oscarpistorius said towards end of Friday he "knelt down". HUGE, I hope #Gerrienel picked it up. He had his prosthesis on."

Some of the tweets border on defamation. Although a tweet like "Still incredulous that #BarryRoux +team not know/undrstnd parallax error. Or was this rank dishonesty in court?" may lead to a defamation suit on grounds of innuendo, it is unlikely that the source of the message can be traced in cyberspace.

Fans of the accused or any famous individual who is involved in a polemic matter can voice their support as illustrated by the following tweet: "Osci Love you stax my HERO !! Believe it was a tragic accident Be strong and know you are blessed." The following call for support has a philosophi-

cal ring to it as well as a link to a website: "If I were to remain silent, I'd be guilty of complicity" - Einstein - Show support for Oscar at: http://support-foroscar.wordpress.com/ #OscarPistorius."

As could be expected in such an emotive case, some of the tweets contains hate mail. Many tweeters call for Oscar to admit to murdering the deceased. This following example contains abuse: "Dear Oscar. Just admit you intended to kill her. You're wasting my precious bloody tax money, you bastard."

Last but not least, the most predictable punchline: "The Oscar for the best actor in a dramatic role goes to....#OscarPistorius...slow clap..."

3.1.3 A grey area

The question arises whether there is a grey area where journalists who work for a news corporation can tweet in their personal capacity. The Twitter profile of one of the most influential journalists in the country, Adriaan Basson, reads: "Netwerk24 editor-in-chief / hoofredaktuer. Author of 'Zuma Exposed' (Jonathan Ball). Digital first. Views are my own."

Until the courts have not ruled on this issue, it will be clouded by legal uncertainty.

4. Impact on the court of public opinion

4.1 Professional journalists

It has been established that the modern court of public opinion consists of a wide array of input from the formal media, public participation fora, and the social networks. In this paper two sets of input from the twitterati was analyzed. Although the samples of tweets that were drawn are two small to warrant any scientific quantification, it makes sense to inspect the impact of metajournalism on the distribution of the selected tweets.

The controversial media personality, Gareth Cliff, tweeted "Let me put it to you (again) - latest blog on the #OscarPistorius trial http://www.garethcliff.com/blog/?p=491." Cliff tweeted to point his followers to his latest blog. Although nobody engaged in conversation with him, he got 88 retweets and 66 favourite nominations.

A tweet from the British TV channel, Sky, got 90 retweets and 46 favourite nominations. It read: "#oscarpistorius has stumbled and stuttered

and wriggled and retracted and added all morning. Not been a pretty sight".

As could be expected, a tweet on the contoversial verdict that was later overturned on appeal, generated the most metajournalism. It generated 18 converstations, 747 retweets, and 1268 favourite nominations.

4.2 Citizen journalists

The tweets from citizen journalists, although more quirky, drew very little metajournalism. The tweet, "Why did OP shout/wail for help, when he had Frank on the premises, surely calling the live in housekeeper would be obvious #OscarPistorius," generated 10 conversations, 4 retweets, and 2 favourite nominations.

The only other tweet that impacted on all the categories of metajournalism read "#OscarPistorius In his written statement. Oscar refers to himself ('I') 82 times. He refers to Reeva just 6 times. Surely that's moody?" Five conversations, 4 retweets, and 7 favourite nominations were recorded.

5. Conclusion

The paper provides clear evidence that the historic concept of the "court of public opinion" has been redefined by the advent of the internet and the social media. A domain that was previously controlled and monopolized by the formal media has now been made accessible to the general public. Members of the public who act as citizen journalists can now constructively contribute to the public, as well as the media agenda. Although the formal media supported by metajournalism still remains a tour de force, the cititizen journalists hold their own through unconventional style, strong opinions, and bold conversations.

6. References

1. Hauser, Gerard A. (1999). *Vernacular Voices: The Rhetoric of Publics and Public Spheres*. Columbia: University of South Carolina Press. p. 61.
2. Habermas, Jürgen. (1991). *The Structural Transformation of the Public Sphere. An Inquiry into a Category of Bourgeois Society*. Cambridge, MA: MIT Press.

3. Goldberg, G. (2010). Rethinking the public/virtual sphere: The problem with participation, in *New Media & Society,* 13(5), pp. 739–754, retrieved from DOI: 10.1177/1461444810379862 nms.sagepub.com.

4. Anon. (1994). The Court of Public Opinion, in *Maclean's, 107 (27),* p. 54, 7/1/94.

5. Hudson, H.P. (1994). The Court of Public Opinion, in *Public Relations Quarterly,* 39, 2.

6. Bady, A. (2014) . There is no such thing as the Court of Public Opinion (but maybe there should be), in *The New Inquiry. Retrieved from* http://thenewinquiry.com/blogs/zunguzungu/.

7. Schneier, B. (2013). The Court of Public Opinion is about mob justice and reputation as revenge, in *Wired,* 26 Feb. 2013, retrieved from http://www.wired.com/2013/02/court-of-public-opinion/.

8. Palmer, E. (2014). Oscar Pistorius: PR team creates Twitter account to reveal "truth" during Reeva Steenkamp murder trial, in *International Business Times,* retrieved fro*m* http://www.ibtimes.co.uk/oscar-pistorius-pr-team-creates-twitter-account-reveal-truth-during-murder-trial-1437738**.**

9. Howden, D. and Burrel, I. 2013. Trial by media of Oscar Pistorius: facts, guesses and spin surround Reeva death, in *The Independent, 19 Feb. 2013,* retrieved from http://www.independent.co.uk/news/world/africa/trial-by-media-of-oscar-pistorius-facts-guesses-and-spin-surround-reeva-death-8500370.html.

10. Harper, A. (n.d.). Citizen journalism vs. professional journalism, in *Journalism: The Future,* retrieved from https://journalismthefuture.wordpress.com/citizen-journalism-vs-professional-journalism/.

11. National Press Club. 2015. *Oscar Pistorius Trial Commemorated as Newsmaker of the Year for 2014.* 15 May, 2015, retrieved from http://www.nationalpressclub.co.za/releases/20150515.php.

12. Harvard Kennedy School. (2016). *Journalism Ethics in the Digital Age: A Model/Open Source Syllabus,* retrieved from http://journalistsresource.org/syllabi/journalism-ethics-digital-age-syllabus#sthash.2Lbcm0xr.dpuf.

13. Gillmor, D. (2009). *We the Media. Grassroots Journalism by the People, for the People.* Cambridge, MA: O'Reilly Media.

14. Friend, C. & Singer, J.B. (2007). *Online Journalism Ethics.* London: Routledge.

15. Silverman, C. (2012). How CNN's iREPORT verifies citizen content, in Poynter, 26 Jan. 2012, retrieved from http://www.Poynter.org/2012.

16. Goode, L. (2009). Social news, citizen journalism and democracy, in *New Media & Society,* vol 11(8), pp. 1287 – 1305, DOI: 10.1177/1461444809341393.

17. boyd, D., Golder, S. & Lotan, G. (2010). Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter, HICSS-43. IEEE: Kavai, HI, January 6, available at www.danah.org/papers/tweettweetretweet.pdf.

18. Alejandro, J. (2010). *Journalism in the age of Social Media.* Oxford: University of Oxford. Reuters Institute for the Study of Journalism.

19. Krotoski, A. (2011). What effect has the Internet had on journalism, in *The Guardian*, 19 Feb. 2011.

20. Thrivehive. (2014). *How to tag somebody on Facebook and Twitter,*22 April 2015, retrieved from http://Thrivehive.com/how-to-tag-someone-on-Facebook-Twitter.

21. Lippman, W. (1922). *Public Opinion*. New York: Harcourt, Brace & co.

22. Boeyink, D.E. & Borden, S.L. 2010. Making Hard Choices in Journalism Ethics. London: Routledge.

23. Zapiro. (2014). Right to a fair trial vs, public's right to know, in Mail & Guardian, 27 Feb. 2014.

Secrecy and Publicness in Digital Democracies: The Netzpolitik.org Case from Multiple Legal Perspectives

by Tobias Keber[1]

1. Introduction

According to common state practice, there is a form of legislation devoted to the protection of state secrets in roughly all national criminal code(s).[2]Hence, from the international law perspective, there is a "right to privacy for states". Arguably, the opposing concept (maximum transparency of state action) was first advocated by Immanuel Kant. In the second appendix of his writing "Zum ewigen Frieden" (Perpetual Peace) Kant underlined the "transcendental principle of the publicity of public law".[3] Kant argued that «All actions relating to the right of other men are unjust if their maxim is not consistent with publicity». This indicates that Kant highlights the human rights dimension of publicity.[4]

1 Tobias Keber, Lawyer and since 2012, Professor at the Stuttgart Media University, Chair for Media Law and Policy, Faculty Electronic Media. Lecturer (Internet and Media Law) at the Mainz Media Institute and the University of Koblenz-Landau. In honorary capacity, Tobias Keber is Co-Head of Institute for Digital Ethics and Head of the Scientific Advisory Board of the German Association for Data Protection and Data Security (GDD). For details and publications see: http://www.rechtsanwalt-keber.de.

2 For an overview see Larsen/Atcherley, Freedom of expression-based restrictions on the prosecution of journalists under state secrets laws: a comparative analysis, 50 J. Int'l Media & Entertainment Law 49-109.

3 "Alle auf das Recht anderer Menschen bezogene Handlungen, deren Maxime sich nicht mit der Publicität verträgt, sind Unrecht. Dieses Princip ist nicht bloß als ethisch (zur Tugendlehre gehörig), sondern auch als juridisch (das Recht der Menschen angehend) zu betrachten."English text of the second appendix available at: http://www.constitution.org/kant/append2.htm. For an interpretation of Kant's concept of publicity, see Wegener, Der geheime Staat, p. 143.

4 For a similar approach (no protection of state secrets), see the hacker ethics, providing inter alia: "Make public data available, protect private data." Ethics available via the Chaos Computer Club via: http://dasalte.ccc.de/hackerethics?language=en. See also Murray, Should states have a right to informational privacy? in: Klang / Murray (ed.)

A government's desire to keep information secret on national security grounds may conflict with the public's right to know. The latter may be interpreted as being complementary to the freedom of the press. Access to information for the public is certainly a key element of democratic participation. The right to know enables public scrutiny of state action. It is a human right which -in the sense of a liberal understanding of fundamental rights- obliges the state to do or to refrain from certain actions. The state has the duty to protect human rights. In certain circumstances, this includes keeping information secret in order to protect people, as a part of the national security interest.

The potential threat for state secrets was emphasized in discussions regardingthe whistleblower platform Wikileaks. For example, in 2010, Amnesty International and three other prominent rights groups called on the whistleblower website to expunge the names of Afghans mentioned in the war logs because of the fear of being targeted by insurgents. In November 2009, WikiLeaks published the '9/11 messages', a massive archive including thousands of text messages sent on September 2001 in the wake of the terrorist attacks on New York and Washington.

Striking the right balance between transparency and secrecy is essential for modern (digital) Democracies.The Netzpolitik.org case perfectly exemplifies the problem.

2. The Netzpolitik.org case

2.1 Facts of the case

Netzpolitik.org is a Berlin-based digital rights blog founded in 2002 covering topics like mass surveillance, open source software, data protection, privacy and net neutrality. On July, 30th 2015 the editors of the blog, Markus Beckedahl and Andre Meister received a letter from the Federal Public Prosecutor (German: Generalbundesanwalt). The Generalbundesanwalt is representing the federal government of Germany at the Bundesgerichtshof, the federal court of justice. The Generalbundesanwalt, at that time Harald Range, has primary jurisdiction in cases of crimes against the state and

Human Rights in the Digital Age, pp. 191 ff.

in his letter confirmed ongoing investigations againstNetzpolitik.org. To be more precise, Beckedahl, Meister and their unknown sources were suspected of Treason. The letter from the Generalbundesanwalt[5] was based on complaints from the Federal Office for the Protection of the Constitution (Verfassungsschutz). The Verfassungsschutz argued that Netzpolitik.org had published two articles[6]disclosing classified documents from the Verfassungsschutz which is Germany's domestic intelligence agency.

The first article (original title: "Secret Moneyrain: Federal Office for the Protection of the Constitution is working on mass analysis of internet content") had been published by netzpolitik.org in February 2015 and reported on the German government's plans to collect and monitor troves of Internet and social media data. The Article also indicated that there was a secret budget for the government´s programme. The article asserted that the government's plans mirrored the mass data acquisition by the NSA in the US. In order to substantiate netzpolitik.org´s critical viewpoint, the article included the link to a pdf-file containing the full text of a leaked secret surveillance budget from 2013.

The second article (original title: "Secret unit group: we are presenting the new Federal Office for the Protection of the Constitution-Unit concerning the extension of internet surveillance") had been published by netzpolitik.org in April 2015 and reported on the German secret service's plan to set up a new Internet surveillance department dedicated to improving and extending the government's mass surveillance capabilities. The German version of the article included the full text of a leaked document describing the government's plans for the new unit officially called "Extended Specialist Support Internet" department.

According to the Federal Public Prosecutor, the disclosure of those documents gave rise to the suspicion of treason appropriate to Section 94 Para 1 Number 2 of the German Penal Code. This provisions stipulates that "Whosoever […] allows a state secret to come to the attention of an unau-

5 The original letter and also an English translation of the text is available at: https://netzpolitik.org/2015/suspicion-of-treason-federal-attorney-general-announces-investigation-against-us-in-addition-to-our-sources/.

6 English abstract of the articles available at: https://www.eff.org/deeplinks/2015/07/german-investigation-netzpolitik-coverage-leaked-surveillance-documents-confirmed.

thorised person or to become known to the public in order to prejudice the Federal Republic of Germany or benefit a foreign power and thereby creates a danger of serious prejudice to the external security of the Federal Republic of Germany, shall be liable to imprisonment of not less than one year."[1]

Also on July, 30th Netzpolitik.org published an article under the headline "Suspicion of Treason: Federal Attorney General[2] Announces Investigation Against Us." They informed their readers about the investigations and made the original letter of the Federal Public Prosecutor available online (full text).

Shortly after, 1500 journalists, citizens and civil society representatives signed a statement[3] declaring that the investigation for treason and their unknown sources is an attack against the free press, and demanding to put an end to it. A demonstration supporting Netzpolitik.org was organised on 1 August in Berlin. In social media, people posted under #landesverrat. The (traditional) media covered the case. For example, the Frankfurter Allgemeine Zeitung asked why the grave charge of treason had been employed "to train the big guns of the judiciary on the poor bloggers of netzpolitik.org."[4]

Following the protests, the Generalbundesanwalt decided to put the investigation on hold, and stated that he would "await the results of an internal investigation into whether the journalists had quoted from a classified intelligence report, before deciding how to proceed." In his press-statement[5] he harshly criticised «political influence» on the suspected treason investigation and said that he had been pressured into putting the inquiry on hold by Justice Minister Heiko Maas.

On the 5th of August, after consultations with Chancellor Angela

1 An English Version of the German Penal Code is available at: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p0973.

2 Netzpolitik.org translates "Generalbundesanwalt" as "Federal Attorney General".

3 The petition is avalable at https://netzpolitik.us/statement/.

4 See also "German Journalists Celebrate as Treason Inquiry Is Dropped", New York Times, Aug. 10th, http://www.nytimes.com/2015/08/11/world/europe/germany-treason-reporters.html?_r=0.

5 In German available at http://www.generalbundesanwalt.de/de/showpress.php?themenid=17&newsid=560.

Merkel's office, Justice Minister Heiko Maas dismissed Harald Range. Less than a week after Range's dismissal, the now acting Federal Public Prosecutor announced that he had concluded, in agreement with the Ministry of Justice, that the leaked documents did not constitute state secrets, and that the investigation will be dropped.[6]

2.2 Aftermath - Donations up, press freedom down?

For Netzpolitik.org, the case meant a monetary blessing. Donations had poured in to help the bloggers' legal battle. In August, Netzpolitk.org had received 50.000 Euro in a few days. The year before it was 180.000€ in total. From the legal science perspective, one may regret that through the dropping of the accusations, possible proceedings in front of the Federal Constitutional Court in Germany became moot. Unfortunately, there is no second (third) Spiegel case. Anyway, the case definitely left scars within Germany's public discourse. Against this background, it is not sure that Germany will rank 12th again in the forthcoming World Press Freedom Index.[7]

3. Treason, State secrets and German (case) law

3.1 Provisions in the German Criminal Code

Section 93 GCC provides the legal definition of "state secret" stating:

(1) State secrets are facts, objects or knowledge which are only accessible to a limited category of persons and must be kept secret from foreign powers in order to avert a danger of serious prejudice to the external security of the Federal Republic of Germany.

6 Järvinen, Netzpolitik.org case: Prosecutor dismissed, inquiry dropped available at https://edri.org/netzpolitik_case_prosecutor_dismissed_inquiry_dropped/.

7 The Reporters Without Borders World Press Freedom Index ranks the performance of 180 countries according to seven criteria that include media pluralism, independence, respect for the safety and freedom of journalists as well as the the legislative, institutional and infrastructural environment in which the media operate. For the index see http://index.rsf.org/#!/. Details for Germany http://www.hlci.de/wp-content/uploads/2015/08/HLCI-Request_for_Inquiry.pdf. Note of the editor: the author is right, Germany lost the 12th place in 2016 and fell to the 16th. See rsf.org/en/ranking.

The Provision relevant in the Netzpolitik.org-case is treason in Section 94 GCC which states:

(1) Whosoever

1. *communicates a state secret to a foreign power or one of its intermediaries; or*
2. *otherwise allows a state secret to come to the attention of an unauthorised person or to become known to the public in order to prejudice the Federal Republic of Germany or benefit a foreign power and thereby creates a danger of serious prejudice to the external security of the Federal Republic of Germany, shall be liable to imprisonment of not less than one year.*

Section 353b GPC sanctions the "breach of official secrets and special duties of confidentiality" stating:

(1) Whosoever unlawfully discloses a secret which has been confided or become known to him in his capacity as

1. a public official
2. a person entrusted with special public service functions or
3. a person who exercises duties or powers under the laws on staff representation

and thereby causes a danger to important public interests, shall be liable to imprisonment not exceeding five years or a fine. If by the offence the offender has negligently caused a danger to important public interests he shall be liable to imprisonment not exceeding one year or a fine.

3.2 Secrets and FCJ/FCC-decisions

In the Netzpolitik.org case, one can safely argue that the information concerned "facts only accessible to a limited category of persons". But was it also facts that "must be kept secret from foreign powers in order to avert a danger of serious prejudice to the external security of the Federal Republic of Germany"? In order to answer this question, the relevant decisions of the German Federal Court of Justice FCJ and the Federal Constitutional Court

FCC have to be taken into account.[8]

According to a decision of the Federal Court of Justice from 1965[9], this disclosure of secrets may be legitimate under certain, very strict conditions. The accused (Mr. Werner Pätsch) had been an employee of the German Domestic Intelligence Agency. During his work, he discovered that the Agency practiced illegal wiretapping. He was reluctant to confide in his superiors as they, in his view, constituted a clique of individuals that had worked for the former Secret State Police (Gestapo). Pätsch therefore contacted a lawyer and later informed the press (the Spiegel) regarding the illegal wire tappings.[10] Against this background, he was accused of having disclosed secrets in the sense of Sections 93 ff and 353b of the Criminal Code. In the decision, the Federal Court of Justice made it clear that Article 5 of the German Constitution provides the right to reveal serious irregularities in agencies in order to remedy abuses. If this information concerns state or official secrets, the person disclosing it must limit the information to that which is strictly essential to end the abuse. Furthermore, before communicating with the public, superiors within the agency must be contacted. In exceptional cases where the constitutional order is seriously infringed, the public may be directly informed.[11] Against this background, Pätsch was convicted but the sentence was lenient (suspended sentence).

In the Wallraff/Bild Decision,[12] the Federal Constitutional Court made clear that the propagation of unlawfully acquired information falls within the protective scope of the freedom of the press.[13] The Court also turned

8 In that regard see also Keber, Secrecy, Privacy, Publicity, Transparency in: Dörr, Dieter/ Weaver, Russell L. (eds.): The Right to Privacy – Perspectives from Three Continents. Berlin, Boston: de Gruyter, S. 344-356.

9 Federal Court of Justice, ruling of 8. 11. 1965 - 8 StE 1/65.

10 See Spiegel, Article 40/1963. Online available at:http://www.spiegel.de/spiegel/print/d-46172126.html.

11 Federal Court of Justice, decision of 8. 11. 1965 - 8 StE 1/65.

12 BVerfGE 66, 116, 1 BvR 272/81, English text available at http://www.utexas.edu/law/academics/centers/transnational/work_new/german/case.php?id=638.

13 The case related to the question of whether a civil-court decision is compatible with freedom of the press when the civil-court decision condones the publication of information stemming from the editorial area of an organ of the press (Bild newspaper) that was acquired by an individual (Günter Wallraff) through deception as to his identity and intentions. Journalist Wallraff had worked undercover as "Hans Esser" in the Edi-

to potential limits and the significance of the concerned knowledge in informing the public and for the formation of public opinion.

In its groundbreaking Spiegel decision,[14] the Federal Constitutional Court carefully balanced the necessity of military secrecy and State security as well as the freedom of the press. In an article published in 1962 called «Bedingt abwehrbereit» («prepared for defense to limited extent») the sorry state of the German Army (Bundeswehr) had been uncovered on the basis of secret military information.[15]The publisher of the magazine, Rudolf Augstein was accused of treason (Landesverrat)[16] and the editorial offices of Spiegel were searched. The Constitutional Court, reviewing the constitutionality of these acts, stated in the Spiegel decision:

> *"…the significance of the published facts, etc. are to be taken into consideration both for the potential opponent and for the formation of political opinion on a case-by-case basis; the threats to the security of the nation that might arise from publication are to be balanced against the need to be informed of important events, including in the area of defense policy."*[17]

The eight judges[18] delivering the ruling each balanced the affected legal in-

torial Office of the "Bild" Newspaper in Hannover. He later reported his impressions in a book in which he dealt critically with journalistic methods, editorial work and the contents of the "Bild" Newspaper.

14 Federal Constitutional Court (BVerfG), Decision of 05.08.1966, Az. 1 BvR 586/62, 610/63 and 512/64 (BVerfGE 20, 162, Spiegel), English Text of the Spiegel decision available at: http://www.utexas.edu/law/academics/centers/transnational/work_new/german/case.php?id=651.

15 A transcript of the original article is available at http://www.spiegel.de/spiegel/print/d-25673830.html.

16 For the indictment, see Federal Court of Justice, Decision of 13.5.1965, 6 StE 4/64, NJW 1965, 1187.

17 Federal Constitutional Court, FN. 35 (Spiegel).

18 The Federal Constitutional Court consists of sixteen justices, half of them elected by the Bundestag and the other half elected by the Bundesrat. The Court decides through the Plenary, a Senate or a Chamber. The Plenary (all sixteen members of the Court) decides, should one Senate wish to depart from the legal opinion of the other. Usually, one of the two Senates (with eight members each) or a chamber (three members each and there are three chambers in each Senate) decides. The Chambers primarily determine whether a constitutional complaint is to be admitted for decision.

terests quite differently. Four judges ruled against a violation of press freedom, giving State security interests the right of way.[19] The other four judges (stalemate) argued *inter alia*:

> *"the uncovering of fundamental weaknesses in defense readiness may in the long term be more important than secrecy, despite the military detriment to the good of the Federal Republic that this might initially entail; the public's reaction normally will prompt the responsible State organs to initiate the required remedial measures."*[20]

The voting result was clearer in Cicero, a case with quite a similar factual background.[21] In 2005, seven judges voted in favor of a violation of press freedom.[22] The Federal Constitutional Court stated that, in the view of press freedom, the mere publication of an official secret by a journalist within the meaning of section 353b of the Criminal Code was not sufficient to justify the suspicion that the journalist had aided and abetted a breach of official secrecy.[23]

As a result of the Cicero affair, Section 353b(3a) of the Criminal Code was introduced, stipulating that journalists are not guilty of complicity to

19 Section 15(4), third sentence of the Law on the Federal Constitutional Court (BVerfGG) states: "If the votes are equal, the Basic Law or other Federal law cannot be declared to have been infringed."

20 Federal Constitutional Court, FN. 35 (Spiegel).

21 In April 2005, the monthly political magazine Cicero had published an article about Islamic terrorist Abu Musab al Zarqawi in which it cited a confidential leaked internal report of the Federal Criminal Police Office (Bundeskriminalamt). Shortly afterwards the editorial offices and the private home of Bruna Schirra (author of the article) were searched and material was confiscated. The searches had been based on the suspicion that the journalist would be an accessory to the breach of official secrecy committed by the journalist' s unknown "source".

22 Decision of the Federal Constitutional Court of 27.02.2007, Az.: 1 BvR 538/06, 1 BvR 2045/06 (Cicero).

23 Rather, specific factual evidence was required to show that the person concerned (the informant) had disclosed the secret aiming it´s publication. Otherwise, as the judges further stated, there was a risk that public prosecutors could instigate preliminary proceedings against editors or journalists just in order to discover the identity of the source. Federal Constitutional Court, Cicero, FN. 41. For a discussion of the case see Schmidt-De Caluwe, Pressefreiheit und Beihilfe zum Geheimnisverrat i.S. des § 353b StGB - Der Fall "Cicero" und die Entscheidung des BVerfG, NVwZ 2007, p. 640.

commit treason if their action is restricted to the receipt, processing or publication of the secret even if they got it from a civil servant who has a special duty of secrecy.[24]

The considerations in the Spiegel-Case, especially taking into account its unique historical context (cold war, delicate situation i.e. cuba crisis) lead to the assumption that the information in the Netzpolitik.org case did not constitute a state secret. The information was not that sensitive (budget questions, surveillance capabilities) and it is hard to argue that the Bloggers had the intention to prejudice the Federal Republic of Germany. It would also be daring to argue that the publication created a danger of serious prejudice to the external security of the Federal Republic of Germany. Hence, the new federal prosecutor was surely right when he dropped investigations.

4. A hypothetical case study

Assumed, investigations in Germany were dropped and the bloggers were found guilty of treason. Suppose (not very likely), even the FCC would have confirmed the conviction. The bloggers from netzpolitik.org could have filed an individual complaint before the European Court of Human Rights arguing that Germany infringed their freedom of expression guaranteed in the European Convention on Human Rights. What would happen next?

4.1 ECHR and freedom of expression

The European Convention on Human Rights is an international Human Rights Treaty which entered into force in 1953.[25] The Treaty obliges the 47 Member States of the Council of Europe[26] to secure certain fundamental

24 Section 353b GCC states:Breach of official secrets and special duties of confidentiality (3a) Acts of aiding by a person listed under section 53(1) 1st sentence No 5 of the Code of Criminal Procedure shall not be deemed unlawful if they are restricted to the receipt, processing or publication of the secret or of the object or the message in respect of which a special duty of secrecy exists.

25 Information documents concerning the ECHR and the ECtHR are available via http://echr.coe.int/Pages/home.aspx?p=court&c=#newComponent_1346149514608_pointer.

26 The Council of Europe must not be confused with the European Council and the

civil and political rights. In order to ensure the effective enforcement of those obligations, the convention also established the European Court of Human Rights (ECHR)[27]which is an international court based in Strasbourg, France. Individuals[28] may lodge a complaint arguing that a member State has breached the convention. The judgments of the ECHR are binding: the countries who lost have to comply. German administrative and judicial organs have a duty to take into account the European Convention on Human Rights and the jurisprudence of the European Court for human rights.[29] The Court is not empowered to overrule national decisions or annul national laws, but if the Court finds that there has been a violation, it may award the individual a "just satisfaction". This is a sum of money in compensation for certain forms of damage. The execution of the Court's judgments is supervised by the Committee of Ministers of the Council of Europe.[30]

4.1.1 Article 10 ECHR and the doctrine of proportionality

Article 10 of the European Convention on Human Rights provides the right to freedom of expression and information. The provision states:

Council of the European Union. The Council of the European Union (often referred to as the Council) represents the executive governments of the 28 EU's member states. Together with the Parliament, the Council forms the legislative body of the European Union. The European Council has no formal legislative power and sets the EU's policy agenda. The members of the European Council are the heads of state or government of the 28 EU member states, the European Council President and the President of the European Commission.

27 The ECHR must not be confused with the European Court of Justice (the highest court of the European Union) which is based in Luxemburg.

28 Inter-state cases are also possible, but they are rare. For a list of those cases see http://www.echr.coe.int/Documents/InterStates_applications_ENG.pdf. For example, there are actually three inter-state applications lodged by Ukraine against Russia.

29 For the legal significance of ECtR judgments within German national law, see the Görgülü Case, ECHR, No. 74969/01, Judgement of 26 February 2004. For a discussion of this case see Lübbe-Wolff ECHR and national jurisdiction - The Görgülü Case, HFR 2006, Beitrag 12, p.1.

30 The Committee of Ministers is made up of the ministers of foreign affairs of each of the 47 member state or their permanent diplomatic representatives in Strasbourg. http://www.coe.int/T/CM/aboutCM_en.asp.

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

There is a substantial body of case-law regarding this article.[31] The Court has described freedom of expression as "one of the basic conditions for the progress of democratic societies and for the development of each individual".[32] But, as Article 10 para. 2 makes clear, the freedom of expression and information is not absolute. The state may legitimately interfere with that freedom under three conditions:

1. restrictions must pursue one of the aims explicitly mentioned in article 10 para. 2,
2. any restriction on freedom of expression must be prescribed by law and most important
3. any restriction must be "necessary in a democratic society.

The first condition means that the Member State must show that the national provision claimed to legitimise the interference pursued one of the aims listed exhaustively in Article 10 para. 2. With respect to the second

31 See Council of Europe Publishing, Human rights files, No. 18, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-18(2007).pdf; European Audiovisual Observatory (Ed) Freedom of Expression, the Media and Journalists: Case-law of the European Court of Human Rights, IRIS Themes, Vol. III (2015) http://www.obs.coe.int/en/iris-themes.

32 *Handyside v. the United Kingdom*, judgment of 7 December 1976, Series A No. 24 para 49. (5493/72) [1976] ECHR 5.

condition (prescribed by law/in accordance with the law) the Court made clear that this does not just mean some basis in the law of the country concerned. Generally, the law must be adequately accessible and sufficiently clear in its terms in order to enable the citizen to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[33] Also, national law has to provide a sufficient element of control over the relevant decision-maker in order to avoid the exercise of arbitrary action.[34]

The third condition incorporates the principle of proportionality. This principle requires that there is a reasonable relationship between a particular objective to be achieved and the means used to achieve that objective. In other words, the question is whether there is "a fair balance" between the general and individual interests. In its case law, the Court also asks whether a particular measure could be achieved by a less restrictive means. Regarding measures interfering with freedom of expression, the ECHR's proportionality test addresses, whether there is a pressing social need[35] for the relevant restriction and whether the particular restriction corresponds to that need.

The doctrine of proportionality marks the heart of the Court's investigation into the reasonableness of restrictions but there is a complex interaction with the principle of judicial restraint.

4.1.2 Strict scrutiny v. margin of appreciation

In general, the Court does not deny that member states have some discretion in assessing what is necessary ("margin of appreciation"). On the other side, this cannot mean that there is no supranational review.[36] Hence, the exact scope (wide or narrow) of the margin of appreciation is subject to ac-

33 Sunday Times, App No. 6538/74, judgment of 26 April 1979, para 49, Silver and Others judgment, App. Nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, judgment of 25 March 1983, paras. 87 and 88.

34 *Malone v. the United Kingdom*, no. 8691/79, judgment of 2 August 1984 para 67.

35 *Handyside v. UK*, no. 5493/72, 7.12.1976.

36 For further discussion, see Shany, Toward a General Margin of Appreciation Doctrine in International Law? (2005) European Journal of International Law 16 (No. 5), p. 907.

ademic discussion and manifold case law.[37] It is undisputed that the scope varies according to the specific aim.

One may safely argue that national security interests require a wide margin because they are highly sensitive objectives and are closely related to State sovereignty, one of the basic principles of international law. This is the reasoning in some ECHR Cases. For example, the Court stated in the *Klass v. Germany* case[38]: "it is not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field."[39] In another decision, the Court noted that the margin available to the State in assessing the pressing social need [...] and in particular in choosing the means for achieving the legitimate aim of protecting national security, [is] a wide one."[40]

On the other hand, the Court has also stated: "Where there has been an interference in the exercise of the rights and freedoms guaranteed in paragraph 1 of Article 10, the supervision must be strict, because of the importance of the rights in question; the importance of these rights has been stressed by the Court many times. The necessity for restricting them must be convincingly established".[41]

37 Brems, The Margin of Appreciation Doctrine in the Case-Law of the European Court of Human Rights (1996) Heidelberg Journal of International Law 56, p. 240. See also Smith, The Margin of Appreciation and Human Rights Protection in the 'War on Terror': Have the Rules Changed before the European Court of Human Rights, Essex Human Rights Review Volume 8 Number 1, October 2011, p. 130.

38 In *Klass v. Germany*, 2 EHRR 214, 6 September 1978, the applicants challenged German legislation as it permitted surveillance measures without obliging the authorities in every case to notify the persons concerned after the event, and in that it excluded any remedy before the courts against the ordering and execution of such measures. The Court, aware of the increasing threat of terrorism, accepted that the existence of some legislation granting powers of secret surveillance was, under exceptional conditions, necessary in the interests of national security and/or for the prevention of disorder or crime. On the other hand, it held that States may not, in the name of the struggle against terrorism adopt whatever measures they consider appropriate. Adequate and effective guarantees against abuse of surveillance measures were essential.

39 Klass v. Germany, App. No. 5029/71, (1978) para. 49.

40 Leander v. Sweden, App. no. 9248/81 (1987) para. 59.

41 Autronic AG v. Switzerland, judgment of 22 May 1990, Series A No. 178, para 61. See also *Worm v. Austria*, judgment of 29 August 1997, Reports 1997-V, para 47.

4.2 State Secrets and ECHR case law

If the netzpolitik.org case was an individual complaint before the ECHR, what would have happened? There are some ECHR Decisions which are illustrative for balancing the interest in publishing certain information through the press versus the interest of the State in secrecy.

4.2.1 The spycatcher case: relevant information is already available

In *Observer and Guardian v. UK* and *Sunday Times v. UK* 1992 ("Spycatcher-Cases"), the ECHR found that the prohibition of newspaper publications detailing the contents of a book featuring inside information on the British special services was not in conformity with the freedom of expression. In line with the established body of case law,[42] the Court once more stressed the presses' role as a «public watchdog of democracy». Addressing the question as to whether the prohibition was "necessary in a democratic society", the court denied this necessity because the information (the book) was freely available elsewhere, namely in Australia where the book had been published without any restrictions.[43] Also in the Vereniging Weekblad Bluf! Case[44], the Court held that it was unnecessary to prevent the disclosure of certain information seeing that it had already been made public.[45]

42 See for example ECHR, Goodwin vs. UK, Decision of 27 March 1996, no. 17488/90; ECHR, *v. Hannover v. Germany*, Decision of 24 June 2004, no. 59320/00.

43 *Observer and Guardian v. the United Kingdom*, Decision of 26 November 1991, no. 13585/88.

44 In the spring of 1987 the editorial staff of the left-wing Bluf! came into possession of a quarterly report by the internal security service. Dated 1981 and marked "Confidential", it was designed mainly to inform staff and other officials. It showed that at that time the internal security service was interested in, among other groups, the Communist Party of the Netherlands and the anti-nuclear movement. The editor of Bluf! proposed to publish the report with a commentary as a supplement to issue no. 267 of the journal on 29 April 1987. Later and due to proceedings brought against Bluf! by the internal security service, Bluf's premises were searched and the entire print run of issue no. 267 was seized. The police apparently did not take away the offset plates remaining on the printing presses. Hence, Bluf´s staff managed to reprint the issue and some 2,500 copies were sold in the streets of Amsterdam the next day.

45 *Vereniging Weekblad Bluf! v. the Netherlands* - 16616/90, Judgment 9.2.1995, para 45

4.2.2 The Stoll case: timing and presentation

In the *Stoll v. Switzerland*[46] case, a Swiss journalist filed his sentencing through national courts to pay a fine for having disclosed a confidential report by the Swiss ambassador to the United States in the press. The report was about the strategy to be adopted by the Swiss Government in the negotiations between the World Jewish Congress and Swiss banks. Key element of these negotiations was the subject of compensation due to Holocaust victims for unclaimed assets deposited in Swiss bank accounts.

In *Stoll v. Switzerland*, the Court held that there had been no violation of Article 10. The Court considered it vital to diplomatic services and the smooth functioning of international relations for diplomats to be able to exchange confidential or secret information. However, the confidentiality of diplomatic reports could not be protected at any price. Referring to the Goodwin case[47], the Court also noted that the conviction of a journalist for disclosing information considered to be confidential or secret may discourage those working in the media from informing the public on matters of public interest. The Court speaks about to potential "chilling effect". As a result, the press may no longer be able to play its vital role as a "public watchdog" and the ability of the press to provide accurate and reliable information may be adversely affected.

Balancing the conflicting interests, the Court analysed the exact content of the report and the potential threat posed by its publication. In doing so, the Court made clear that in this case the public's interest in being informed had to be weighed not against a private interest but against another public interest: the interest of the authorities in ensuring a positive and satisfactory outcome to the diplomatic negotiations.[48] Finding that the articles were published in the context of a public debate, the Court also noted that it was vital to diplomatic services and the smooth functioning of international relations for diplomats to be able to exchange confidential or secret information.

The Court noted that it was important to ascertain whether the dis-

46 Eurp. Conv. Prot. Hum Rights. ECHR, *Stoll v. Switzerland*, Decision of 10 December 2007, no. 69698/01.

47 *Goodwin v. The United Kingdom*, 27 March 1996, § 39, Reports 1996−II.

48 *Stoll v. Switzerland*, 115.

closure of the report and/or the impugned articles were, at the time of publication, capable of causing "considerable damage" to the country's interests.[49]In that context the Court attached some importance whether the documents were classified as "confidential" or "secret". According to the Court's reasoning, the time of the publication may also heighten the risk of a potential threat. In the Stoll case, the publication fell in a time where negotiations on the issue of unclaimed assets were in a very sensitive phase. Finally, the Court also examined the way in which the articles had been edited. The Court argued that the vocabulary used was clearly liable to provoke a negative reaction from the other parties to the negotiations, namely the World Jewish Congress, and, in consequence, to compromise the successful outcome of negotiations. For example, the article discovered that the ambassador expressed the view that Switzerland's partners in the negotiations were "not to be trusted" but that it was just possible that "an actual deal might be struck" with them. Furthermore, he described them as "adversaries".[50]

4.3 Article 10 ECHR case law

4.3.1 Freedom of expression and the Internet

As the Grand Chamber of the ECHR in 2015 in the Delfi Case[51] noted, Article 10 of the Convention also applies to the Internet as a means of communication. The Court argued that "in light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally." But, the Court also made clear that the risk of harm posed by content and communications on

49 In the same line of reasoning, the Court in the Vereinigung Demokratischer Soldaten Österreichs und Gubi case argued that prohibiting the distribution of a journal critical of military life to soldiers was disproportionate because the contents of the articles were not a serious threat to military discipline. *Vereinigung Demokratischer Soldaten Osterreichsaund Gubi v. Austria*, no. 15153/89 judgment of 19.12.1994.

50 Eurp. Conv. Prot. Hum Rights. ECHR, *Stoll v. Switzerland*, Decision of 10 December 2007, Application No. 69698/01.Para 135.

51 *Delfi AS v. Estonia*, no. 64569/09, 16 June 2015.

the Internet is potentially higher than that posed by the press.[52]

The unique nature of the Internet has led the Court to establish specific criteria to balance freedom of expression and respect for other rights or requirements. This is not just because of the fast and ubiquitous nature of the internet. Media convergence also plays an important role as the internet is also a distribution channel for audiovisual content. In that context and considering the "duties and responsibilities" of a journalist, the Court reiterated that it is commonly acknowledged that the audiovisual media often have a much more immediate and powerful effect than the print media.[53]

Internet specific "duties and responsibilities" of journalists may also be deduced from the already mentioned Stoll case. The Court argued: "(…) in a world in which the individual is confronted with vast quantities of information circulated via traditional and electronic media and involving an ever-growing number of players, monitoring compliance with journalistic ethics takes on added importance."[54]

4.3.2 Political and commercial speech

Political speech and comments on matters of general interest generally enjoy a high level of protection and generally imply a narrow margin of appreciation.[55] In contrast, the margin of appreciation is broader, where commercial speech is concerned.[56]

4.3.3 Article 10, amateur journalists and NGOs

In *Steel & Morris v United Kingdom*[57], the Government had pointed out that the applicants were not journalists, and should therefore not attract the high level of protection granted to the press under Article 10. The applicants had been involved in an anti-McDonald's campaign. Entitled "What's wrong with McDonald's?" they had produced and distributed a six-page leaflet harshly criticising the company. The Court rejected the argument of

52 *Delfi AS v. Estonia*, para 133.
53 *Delfi AS v. Estonia*, para 134.
54 *Stoll v. Switzerland*, para 104.
55 *Axel Springer AG v. Germany*, no. 39954/08, para 90 and *Maurice v. France*, no. 29369/10, para 125.
56 *Mouvement raëlien Suisse v. Switzerland*, no. 16354/06, para 62.
57 *Steel & Morris v. United Kingdom*, Application no. 68416/01, 15 Feb. 2005 para 89.

the government noting that in a democratic society even small and informal campaign groups, must be able to carry on their activities effectively and that a strong public interest in enabling such groups exists. It explained that individuals outside the mainstream contribute to the public debate. In later decisions, the Court confirmed this approach arguing that civil society organisations monitoring government performance, may have a similar role to the press acting as some kind of social watchdog.[58]

4.3.4 Case law regarding the protection of journalist's sources

According to established case law, another key element of press freedom is the protection of journalist's sources. That means that journalists have a right to refuse to reveal their sources, unless there is an overriding requirement in the public interest. The reason behind that principle is that "Without such protection sources may be deterred from assisting the press in informing the public on matters of public interest."[59] In *Tillack v. Belgium*,[60] the Court emphasised that the right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources. It is part of the right to information, to be treated with the utmost caution. In the similar case *Voskuil v. The Netherlands*[61], the ECHR added that in a democratic state the use of improper methods by public authority brought to light by the journalist and his source is precisely the kind of issue which the public have the right to be informed about. In De *Telegraaf v. The Netherlands*,[62] again reiterating protection of journalist's sources-principle the court also noted the potentially chilling effect an order of source disclosure could

58 *Társaság a Szabadságjogkért v. Hungary*, App. 37374/05, 14 April 2009, para. 27. *Riolo v. Italy*, App. 42211/07 17 July 2008, para. 63. *Vides Aizsardzības Klubs v. Latvia*, App 57829/00, 27 May 2004, para. 42.

59 *Goodwin v. UK,* 27 March 1996.

60 *Tillack v. Belgium*, no. 20477/05, 27 November 2007, para 65.

61 *Voskuil v. the Netherlands*, no. 64752/01, November 2007 para 70.

62 In *De Telegraaf v. The Netherlands* a newspaper had published articles alleging that sensitive information on pending investigations by the Netherlands secret services (AIVD) into drugs and arms dealings had fallen into criminal hands. The journalists, in possession of the leaked files, working for were ordered to surrender the documents, but objected on the grounds that its source might be identifiable from fingerprints thereon.

have on press freedom. The Court stated that such a measure was not compatible with Article 10 unless it was justified by an overriding requirement in the public interest.[63]

4.3.5 Whistleblowing

A series of ECHR-Decisions addresses whistleblowing. This means the exposure of certain information e.g. misconduct, corruption, mismanagement or illegal activity within an organization by a person, usually an internal employee, to the authorities in charge or to the general public. The ECHR stated: "In a democratic system the acts or omissions of government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of the media and public opinion. The interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence."[64] Case by case, the ECHR decided whether the exposure of certain information by a doctor, teacher, geriatric nurse or through Intelligence Service personnel was justified by overriding public interests.[65]

The protection of whistleblowers is also enshrined in the Global Principles on National Security and the Right to Information, the so called Tshwane Principles (Principle 37). Even if these principles which were drafted right here in 2013 are non-binding, the principles reflect a broad consensus as well as internationally agreed standards and good practices. According to these principles information generally should be kept secret only if its disclosure poses a real and identifiable risk of significant harm to a legitimate national security interest (Principle 3). Principle 10 contains a list of categories of Information with a high presumption or overriding interest in favor of disclosure due to their special significance to the process of democratic oversight and the rule of law. This explicitly covers information concerning expenditures for governmental structures and infor-

63 *De Telegraaf v. The Netherlands*, Application no. 39315/06, 22 November 2012, para 131.

64 ECHR Grand Chamber 12 February 2008, Case No. 14277/04, *Guja v. Moldova* and ECtHR 8 January 2013, Case No. 40238/02, *Bucur and Toma v. Romania*.

65 See *Frankowicz v. Poland,* 16 December 2008, *Marchenko v. Ukraine*, 19 February 2009, *Kudeshkina v. Russia* 26 February 2011, *Heinisch v. Germany*, 21 July 2011, *Sosinowska v. Poland*, 18 October 2011, *Bucur and Toma v. Romania*, 8 January 2013.

mation regarding the legal framework concerning surveillance of all kinds (Principle 10E).

5. Conclusion

The Netzpolitik.org case lucidly illustrates the conflict between the government's desire to keep information secret and the public's right to know. After carefully balancing the rights concerned and taking into account the decisions of the FCC in the Spiegel Case, the case law of the ECHR as well as the Tshwane principles, the arguments of the former Federal Public Prosecutor appear to be ill founded.

The articles contained strong protected political speech. After the Snowden disclosures, surveillance issues trigger the highest public interest. Netzpolitik.org functioned as public (social) watchdog and the potential threat for the Federal Republic of Germany was minimal. No other result may be found looking at the circumstances of the disclosure. Neither was the time of the disclosure extraordinary sensitive, nor was the form of the presentation of the article some kind of immoderately sensational.

6. Links

For facts and opinions concerning the Netzpolitk Case see information via EDRI, BBC: German spy leaks website being investigated, eff.org: German Investigation of Netzpolitik For Coverage of Leaked Surveillance Documents Confirmed and Deutsche Welle: German press, politicians criticize 'absurd' Netzpolitik inquiry.

For related legal questions concerning WikiLeaks see Keber, in: Dörr, Dieter/Weaver, Russell L. (eds.): The Right to Privacy–Perspectives from Three Continents. Berlin, Boston: de Gruyter, S. 344-356.

Article 10 Case Law is available via HUDOC. For Article 10 ECHR case law see: Voorhoof, Freedom of Expression, the Media and Journalists. Case law of the European Court of Human Rights, Strasbourg, European Audiovisual Observatory, Iris, 2013, with T. Mc Gonagle (ed.), 404 p., E-Book.

For information concerning the right to know visit right2info.org.

How to Protect Rights by Informing about Rights? Some Remarks about Polish Law

by Agnieszka Góra- Błaszczykowska[1]

1. Introduction

Nowadays information is more valuable than money. Those who have information have power. Therefore, the media, especially social media, are called the «fourth power». They can influence and shape reality because of access to information about the surrounding reality.

With information about the law one may very well affect the use of the law by individuals. However, knowledge and information about the law in Poland are difficult to acquire and understand because of the very complicated way of creating law by the Polish legislator. In Poland we use to say that the law is only for lawyers. Language, used to write acts and provisions is not understandable by ordinary people, but also by lawyers.

Currently in Poland, the meaning of the law has become almost the primary subject of, heated debate and struggle between political factions, the primary topic of interest of the media and a large part of society. The Polish legislation has a habit of being a detailed regulation of all areas of activity and life. Therefore, current legislative activity of the government has been criticized as chaotic, spontaneous and reckless, and not preceded by consultations between the relevant ministries and analysis prepared by professional legislators.

Criticism of this course of action, and the same laws, by media and NGOs is so loud that it affects society. That is why politicians of various opposition parties, part of the media and members of the public openly criticize the actions of the new government and the ruling party. The biggest objection is the lack of information on the financial impact of legislative changes, which usually are calculated in the course of legislative work[2]. The

1 Professor, University of Social Sciences and Humanities, Poland.

2 For example there's no public available detailed calculation on financial consequences

government defends claims against the necessity of these changes, arguing that they result from both the preelection promises and the need to repair defective legislation, introduced by the previous parliament. However, the biggest problem in Poland is a lack of detailed information on planned and implemented legislative changes. This is a great problem for banks, businesses as well as for practicing lawyers and financial advisors.

The average observer of this discussion does not know the facts, but knows how to evaluate them and to take a stand against them. Most of the representatives of the Polish media (hard to call them journalists) are politically involved on different sides. They do not represent the reality, instead of giving the public the facts they give the comments to them. The mode of action of the media in Poland can be illustratively say they do not tell you what happened, but indicate how to assess what happened.

The right to information is one of the most important components of civil rights. The problem is how to inform about the law so that citizens can benefit from this information and properly conduct their own affairs, to decide whether to undertake business, calculate risks and costs thereof; to decide whether to work or improve their education, to ensure the future maintenance of their families.

Information on the law allows the protection of the rights of citizens: the lack of intormation on rights leads to the inability to use the rights and at worst, - to its violations. Lack of knowledge pushes citizen on the margins of society, generates unnecessary costs or lack of income, which would reach a person familiar with the law.

Poland currently places a strong emphasis on information about civil rights: there are many ways to obtain information about various types of rights and it is possible to get it at many levels and in many aspects. Despite the many efforts of governmental and non-governmental organizations in this field, there is still much to do. Not everyone in need of legal information is aware of the many ways to receive information about the law.

In this article I will present the court system in Poland, there is a problem with the identification of the competent court. Then, I will analyse the

on Act about state aid in upbringing children, from February 11, 2016 (Dz.U. z 2016 r. poz. 195), which is called Act 500 because it gives families 500 zloty (PLN) for child mothly (under some specific conditions).

ways of obtaining information on the law in Poland, and entities that deal with providing it.

The next problem, connected with informing about the law, is two different lawyer's corporation who have right to represent parties before the court (advocates and legal advisors), and existing different group of professionals, who can represent parties before court (tax councellors, property managers). The legal system in Poland could be divided into general and personal, precourt and court one. Generally, legal support is given by advocates (barristers) or legal advisors. In some court cases legal support could be given by other profesionals, for example, tax councellors[3]. Of course, the above mentioned professionals' advices are paid.

There is not problem to find professional legal advisors for those, who have money, who's financial status is good. The problem is for people, who's financial status is so bad so they have not money for lawyers and for profesional legal advice.

I will focus on some aspects of the right to information on the law provisions and the ways of using it by Polish law entities. There is many ways of collecting information about law provision in Poland, f.e. both kind of courts existiting in Poland have a duty to inform parties of the hearings about their rights.

2. Polish court system

The Polish judiciary system consists of two different courts: common and administrative. Common courts hear civil and criminal cases. Civil cases mean labour cases, family cases and commercial cases. Administrative courts are a separate branch of the court system. They hear administrative cases such as on environmental protection law, data protection law, construction law, tax law. The material competence between administrative and civil courts is complex and it is sometimes difficult to understand unless on is an expert on the Polish legal system.

Part of the judgments concerns the cases, which under Polish legal system are classified as personal interest ones under the material competence of common courts, and thus were issued by district court, then appeal court,

3 See more in the chapter II concerning polish court system.

and finally by The Polish Supreme Court. The other part of the judgments are issued by district administrative courts and the Polish Supreme Administrative Court. Some of judgments, connected with freedom of expression are issued by common (civil court) and administrative courts, which are also (in some cases) competent in this matter.

It should be underlined that in view of the above duality of the Polish court system, some legal problems- in case of necessity to prosecute a claim in court-will be settled by common or administrative courts. It explains the necessity of analyses of the judgments of two different kind of courts[4]. This analyses should be provided by profesionals, because those, who are not profesional face serious problem with proper understanding the reasons of judgments issued by some courts.

3. Public available information about law (general)

3.1 The role of media in disseminating information about the law

In Poland access to information on the law is possible not only via professional lawyers, but also free of charge. There are a number of websites where everybody can get information on current legislation. This way of getting information is so important, since it does not require financial outlays and is not dependent on the place of residence in search of information. Therefore, the availability of information on the law for anyone, regardless of financial status is essential for the protection of the rights of individual citizens.

The media play important role in Poland in terms of informing about the law and protecting the rights of citizens. Their informative role is not just about presenting information on the Polish legislation in force, but they also make available to the public interesting cases decided by the courts. Some daily newspapers have special pages devoted to legal issues. There are journalists who visit courtrooms and on an ongoing basis draw up press releases. This way, the media publish up to date public information about the current court decisions, the most interesting cases and issued judgments.

The media have a significant impact on the shape of the legislation. In

4 I have already written an article with details about Polish court system for IAPL Stambul Conference Papers, which will be published.

Poland, the media are able to exert such a significant influence on politicians, that in fact they can influence the law.

Lobbying and pressure of media campaign resulted in entry into force the act of proceedings against the persons with mental disorder creating the danger to life, health and sexual freedom of other people, which entered into force in 22 January 2014. In fact the only reason to form this act was "Trynkiewicz case". Mariusz Trynkiewicz is the man who raped and murdered four boys in 1988 and was sentenced to death. Then few years later, the Polish criminal code was changed (amended) and his penalty was converted to 25 years imprisonment. He completed his imprisonment on 11 February 2014.

From the beginning of the year 2014 all Polish media, expecting his release, launched broad campaign against this man, demanding continuation of his isolation from the society.

The above act envisages the possibility of isolation of person accused on sexual children harasment, after termination of his penalty, by putting him into special, closed, medical center or arranging for him police supervision.

General information about the law and the ways of its implementation on specific issues are available on the websites of the entities and bodies such as the Ombudsman, the Ombudsman for Children, the Insurance Ombudsman, the Ombudsman for Patients' Rights, Consumer Ombudsman. These authorities shall inform about the content of the provisions under which they operate, the extent of their competence and how to redress the scope of matters to which they have been called.

Although there are many options and many readily available sources of information about the law, not everyone in need can reach them.

3.2 Early education

The most important issue is education, providing general information on how to behave in a particular legal situation before there is even a violation of law or before there is a need for legal protection. This is a key aspect of general legal education. This education takes place in schools within the subject "Knowlege about society", lined ranging from the secondary junior school through secondary senior school.

Currently, it seems that older children and adolescents have the best

overall knowledge of the law. In schools there are organized talks and lectures on the law, granted by police, lawyers, volunteers of various institutions and NGOs.

This impression on the limited social group having information on the law are not exaggerated, as evidenced by another, put into force laws, to improve the legal awareness of citizens.

Started from January, the 1st, 2016, the brand- new provisions came into force in Polish law related to free of charge legal suport. According to this act provisions, public administration organs are obliged to educate theirs society to improve level of law knowlege, to inform about rights.

The Act provides, inter alia activities aimed at shaping the legal awareness of citizens. According to the Act, public administrations in carrying out their tasks related to public legal education will be obliged to undertake educational activities aimed at enhancing the legal awareness of society.

Tasks which are the subject of discussed issues will be implemented by public interest organizations, as well as institutions offering higher education with the law faculty, professional associations of lawyers, solicitors, notaries, bailiffs and tax advisors - selected in an open tender procedure[5].

A lot of interest in Poland are TV programs to disseminate legal knowledge about the operation of courts and other judicial and civil rights.

3.3 Blogs

In Poland, there are several different blogs, in particular concerning information about the law and how to claim. Most of them are in fact advertorial law firms, for lawyers and legal advisors can not officially advertise, and therefore leads blogs, which provide quasi-legal advice, general advice, thereby encouraging customers to use their services.

4. General information public available (Pre-court information)

4.1 Oficial website Ministry of Justice

Much of the information about the law and about ways of doing things about the legal sense is on the official websites of ministries, particularly

5 Details on this Act is contained in section IV of the text.

the Ministry of Justice. One can get the information on specific laws and other legal acts. It also includes on-line access to land registers and other registers kept by the Ministry. On the website of the Ministry one can also download forms needed to initiate and investigation of cases before the courts.

4.2 Court's websites

Courts in Poland maintain websites with information on the type of caseload, reveal statistics on the number and duration of proceedings. It is important for potential parties have information on costs, because many times their level depends on the decision to open the proceedings. Court costs in Poland are very different depending on the type of case and the court has jurisdiction to hear it. These costs are quite high- when it comes to the civil courts, but e.g. employee or insured claims coming before the labour court and social security do not bear the costs. The costs are not bear by the party seeking alimony before a family court.

On the websites of courts it is possible to download files, someone needs to take action and apply for exemption from court fees and the establishment of legal aid. In offices filing courts application forms are available (on the same subject) as well as eg. legal remedies and other pleadings needed to independently pursue the case by people who are not professional lawyers.

Moreover, the courts maintain websites which provide judgments issued in specific cases, together with the justifications. Despite anonymization they have significant cognitive and informative value of the case-law in a particular type of case. Information about the contents of sentences issued in certain cases, are useful not only for potential sites, but also for scientists who, based on their analysis can lead scientific research.

4.3 Information about law made available by special institution

Started from January, the 1st, 2016, in Poland come into force brand- new provisions in Polish law related to free of charge legal suport.

The act of free of charge legal support from August, the 5, 2015 enabled free of charge legal support to be given by community (borough) or county (district) (art. 8.1). They engage atorney or legal advisor (art. 6.1) and make

a deal with him. This free of charge legal support is given to natural person (according to art. 4.1) for example, whose age is below 26 years or who completed 65 years old, and their financial status is poor, Big Family Card holder[6], combatants, veterans.

According to art. 3. 1 free of charge legal assistance covers among others informing the eligible person on its binding legal status, on the rights it is entitled to, on its obligations, on the ways to solve its legal problems and/or drawing up the letter requesting for the exemption from the court fees or establishing ex-officio representative in the court procedure or establishing advocate, legal advisor, tax councellor or patent advisor in administrative court proceedings. However legal aid does not cover preparation of the court letters in a precourt or court proceedings as well as the letters in the administrative court proceedings (art.3.1.3).

Free of charge legal aid does not cover taxation cases related to business activity, customs, foreign currency and commercial law with the exception of the matters related to preparations for commencing such activity (art.3.2).

Since January 2016, more than 1,500 points throughout Poland, where professionals provide legal assistance had been created. Thanks to the cooperation of the government, local authorities and NGOs the nationwide system guarantee free access to legal advice at the local level, thereby eliminating financial barrier to access to professional legal services too often occurring in Poland. Such a large number of free legal aid points is expected to abolish barriers to obtaining information on rights by people residing outside large cities in Poland. It is because in big cities, as already noted, access to free legal aid is facilitated by the existence of a number of entities and organizations engaged in the providing (legal corporations, arranging "days of free legal assistance", advocates of consumer, patient advocates, student legal clinics).

The fact that free legal assistance is a task assigned to government administration will unify the rules of granting it. Funds for the implementation of tasks comes from the state budget, which guarantees a permanent source of funding. Free legal assistance is granted at the points specified by the local government units.

6 Big family in Poland it is family with 3 and more children.

An important element of the system is NGOs. Because of their experience and achievements, there is a possibility of entrusting them to keep 50% of the free legal aid points. On a national scale the rise in total of more than 1,500 such points is envisaged.

Free legal aid is provided by advocates and legal advisors as well as, in particularly justified cases, applicants[7] authorized respectively – by the legal advisor or advocate providing free legal aid. However, in the points run by non-governmental organizations legal advices can also be provided by tax advisors and legal studies graduates (with at least three years experience).

Free legal assistance will be provided at points in the average rate of 5 days per week for at least four hours a day. Information about a specific location and opening hours of the points to can be found in the Public Information Bulletin county authorities.

Legal aid consists of:

- release of information about the current state of the law, vested rights or incumbent obligations;
- presentation of proposals on how to resolve the legal problem;
- assistance in preparing a draft letter to the extent necessary to grant legal aid (not include the pleadings in the proceedings or prosecutions and letters in the judicial-administrative proceedings - then the person entitled may request the establishment of ex-officio legal aid);
- drafting pleading for exemption from court fees or to appoint a representative from the office.

4.4 Lawyers corporations actions

Corporations Law, unable to advertise, take different actions, aimed at promoting their services. They organize days of granting free legal aid, carried out various forms of legal education in schools in order to familiarize the participants of their rights and possibilities of using them in certain situations.

As already mentioned, these actions are carried out mostly in the cities,

7 Lawyers who intend to obtain advocate or advisor status.

which are the seats of these corporations, and thus in large and medium cities. Residents of small towns and villages, away from larger centers, have limited access to free legal aid and professional lawyers.

4.5 Student legal clinics

In addition, multiple legal clinics at law faculties of universities are run, where also free information about law may be obtained, but essentially it is used only by the inhabitants of the cities, where the departments of law are located. Keeping these centers is beneficial for students who learn in their profession as well as for the people who can benefit from the assistance of experienced lawyers who approve projects writings and tips provided by the students.

4.6 Administrative tax organs duties

Right to be informed on meaning of provision of Polish tax law could be realised by asking Polish tax administration for "individual tax law interpretation" (article 14 b of the Polish Tax Ordinance). This interpretation is binding both for administration tax organ and tax- payer as long, as Administrative court will not eliminate it by issuing the sentence. Unfortunatelly, also administrative tax organ could change it by sending its second one own interpretation, so tax- payer could not be sure how long exactly the validity of this individual interpretation will last.

5. Information about law provisions available for court's proceeding parties

5.1 Information about law made available by court

First, one should note the obligation of the courts, adjudicating in civil matters, providing the parties with instructions about the proceedings. In accordance with art. 5 Polish Civil Procedure Code (PCPC) it is possible should it prove necessary, but the party must appear on without a lawyer, patent attorney or counsel Attorney-General of the Treasury. A similar obligation has been imposed in art. 212 § 2 (PCPC) under which, in case of a justified need, the judge may give the parties the necessary instruction and according to the circumstances draws attention to the desirability of

establishing a legal representative.

In accordance with art. 6 Administrative Court Proceding Code (ACPC) the administrative court, in the event of justified need, gives the parties before the court without a lawyer, tax advisor or patent advisor, the relevant instuctions necessary for the legal proceedings and the consequences of their negligence.

The cited provisions are intended to level the chances of the parties acting without a professional lawyer.

Suggestions and instructions concerning the procedural steps that should be taken on; how and in what timeframe the court should determine the defects in these proceedings as well as what are the legal consequences of failure to remedy these deficiencies within the time limit.

The court instructions must be given in such a way that the party who does not benefit from the assistance of professional lawyer has not been deprived of opportunities to influence the ongoing court case and thus realize their own rights. The regulations do not require the court to instruct the party on action to be taken in case of negligence in order to reduce their impact.

The principle of information in criminal proceedings is governed by article 16 Polish Criminal Procedure Code (CPC). According to its § 1, if the authority conducting the proceedings is obliged to instruct the parties on the obligations incumbent and about their rights, the lack of such instruction or erroneous instruction may not cause negative effects on the process for the defendant or other person to whom it applies.

Pursuant to art.16 § 2 CPC, the authority conducting the proceedings should also, where necessary, provide participants with information about the procedure responsibilities and about their rights also in the cases where the law clearly does not constitute such an obligation. In the absence of such instruction when, in the light of the circumstances of the case it was indispensable, or erroneous instruction, § 1 shall be applied accordingly.

The provision of art. 16 § 2 CPC does not oblige the authorities of the process to ensure the wider interests of the parties, and only a duty to inform them of these rights and duties that are directly connected to the content of published rulings, decisions, actions[8].

8 Judgment of District (second instance) Court in Warsaw - II Penal Departement June

In terms of proceedings in criminal matters, pursuant to art. 386 § 2 CPC, after questioning the accused the judge instructs him of his right to ask questions to the examined persons and to be given explanations for any evidence.

The provisions of art. 386 CPC are repeating the rights of the accused, referred to in the general provision of article 175 § 1 and 2 CPC, in relation to proceedings at the trial. Immediately after the reading of the indictment the judge instructs the accused of the right to provide explanations, the right to refuse to be heard, as well as refusing to answer the questions asked him, and asks him if he admits to the act, and if he wants to make, and what explanations.

In case of need, depending on whether the accused is assisted by counsel and on his personal characteristics, in particular its level of mental development, level of intelligence, and sometimes also other circumstances related to the hearing, that information can and should be more detailed. In particular, often it could be justified to instruct the accused that his has the right and not an obligation to provide explanations and answer the questions. It means that he may: 1) reduce his explanations to some circumstances only and refuse their submission in the rest of ; 2) refuse to answer only some questions; 3) refuse to answer questions of the court or of the individual designated by himselve, but to answer the questions of others, or 4) to respond only to questions of specific person designated by the party- eg. his defender[9].

This right already exists in the course of the investigation. In accordance with art. 175 § 1 CPC the accused should be advised of the right to provide explanations and the right to refuse to answer particular questions or refuse to answer questions without giving reasons.

In the literature highlights the Article 175 § 1 of the CPC imposed on the judicial body the duty to instruct the accused of his rights concerning providing of explanations[10]. This obligation is specified in a number of subsequent provisions of the Code, according to the stage of the proceedings.

7th, 2013 r. number II AKa 163/13.

9 R. Ponikowski in: J. Skorupka, Commentary to art. 386 k.p.k., Legalis 2015.

10 D. Gruszecka in: J. Skorupka, Commentary to art. 175 k.p.k., Legalis 2016.

In the preparatory proceedings the suspect should be instructed on his rights, including the right to provide an explanation, to refuse their submission or to answer the questions, before the first questioning (Art. 300 CPC).

That instruction should be in writing, and its transfer to the suspect should be recorded by submitting his signature. Also on the stage of criminal proceedings Art. 386 § 1 of the CPC obliges the presiding judge to instruct the accused after reading the indictment on his right to provide explanations and the possibility of refusal of their submission.

The accused (suspect) should be instructed not only about the right to refuse to answer or answers to each question and that he can do so without giving reasons for the refusal, but also the fact that this his attitude will have no negative effects on the process for him[11].

However, there is no obstacle to draw defendant's attention that providing explanations may contribute not only to make findings favorable to him, but also to accelerate the completion of criminal proceedings with art. 16 of the CPC.

In the above circumstances the judical body noticing this failure should instruct the accused of his rights while before questioning it should explain to him that the explanations previously provided by the accused do not constitute evidence and only then re-interrogate the accused.

6. Interpretation of the law provisions for professionals

6.1 Introduction

The Polish law system is based on Constitution, acts, codes and others legal acts. There is a general opinion about the poor quality of Polish law, arising from a number of questionable, vague provisions. In 3 December 2015, the Polish Constitutional Tribunal ruled on partial illegality of the act, which has been created (among others) by three judges of this Tribunal[12]. The example given illustrates the complexity of the Polish legislation and the degree of uncertainty as to the correct understanding of the rules by enti-

11 Judgment of the Polish Supreme Court of 4.2.2008 r., III KK 363/07, BPK 2008, No 5, p. 27.

12 See f.e. judgment number K 34/15, D.U. 2015 position 2129.

ties applying the law.

This problem is not a problem only for the Polish judiciary. In the judgment of the European Court of Human Rights of 22 December 2015[13] it was underlined, that the possibility of conflicting judgments is an inherent trait of any judicial system that is based on the principle of adversarial appeal. This feature cannot be regarded as a manifestation of violation of the Convention. Justifications for a national court decisions cannot be considered arbitrary if only because the use of (unclear) law sometimes requires the interpretation and the possibility of decisions being moved under the means of appeal.

Despite the existance of specific acts and regulations contained in them there is uncertainty as to their significance what results in the fragmentation of the case-law of the Polish courts. This situation is assessed very critically especially when we consider that this diversity is also reflected in the jurisprudence of the highest instance courts, i.e. The Polish Supreme Court and the Polish Supreme Administrative Court.

Justification for the discrepancies judgments of Polish courts is constitutionally guaranteed independence of judges, which is a normative basis for jurisdiction in similar cases regardless of already issued judgments. The more it is not surprising the existing divergence in the case law of authorities, adjudicating eg. in tax matters.

The problem is the interpretation not only of individual provisions, but also their relationships. In addition, problems of interpretation have not only ordinary citizens, professional lawyers, but also the most prominent judges adjudicating in the Polish Supreme Court and the Polish Supreme Administrative Court.

6.2 Legal questions

A very high degree of complexity of the legislation makes it possible for the courts of a particular civil case to request for a binding interpretation of the law by the Polish Supreme Court when the court of second instance recognizes the appeal (art.390 PCPC). According to this article, if while recognizing the appeal there is a legal issue rising serious doubts, the court

13 Stanković and Trajković against Serbia, No. 37194/08 and 37260/08.

may submit the issue to be resolved by the Polish Supreme Court, delaying the case.

The Polish Supreme Court is competent to take the case for its recognition or to pass the issue to be resolved in extended composition of the Court. The resolution of the Polish Supreme Court concerning the specific legal issue is binding in the case. Also, the three judges of the Polish Supreme Court may refer the question to the enlarged composition of that court.

According to article 193 of the Polish Constitution, each court may submit to The Polish Constitutional Tribunal a question of law as to the conformity of a normative act to the Constitution, ratified international agreements or statute, if the answer to that question of law will determine an issue currently before the court.

The quoted provision is an example of doubts about the law, not only are the domain of non-professionals, but also the courts of all instances. Provided for in art.193 of the Polish Constitution legal question can ask any court, not only common, but also the Polish Supreme Court and the Polish Supreme Administrative Court.

6.3 Legal issues arising in courts recognizing remedies (other instance- art.390 PCPC and 441 CPC)

As the first one of those rules one should indicate the provisions of art. 390 PCPC and art. 441 CPC allowing the courts of second instance, to present to the Polish Supreme Court the legal issue raising serious doubts that arose in recognition of the appeal. In both types of proceedings, the Polish Supreme Court may refer the legal issue to be resolved in extended composition of this Court (art.390 § 1 sentence 2 of the PCPC and art. 441 § CPC), the Polish Supreme Court may take the case for recognition (art. 390 § 1 PCPC and art.441 § 5 CPC).

Accomplishing intepretation is used until it is changed by other committee of The Polish Supreme Court.

6.4 Legal issues arising in the courts of the highest court - art. 39817 PCPC and art.18ACPC

Highest Instances Courts- the Polish Supreme Court and the Polish Supreme Administrative Court may also submit legal issue to be resolved in

extended composition of the Courts, if this issue emerges when recognizing cassation (Art. 398[17] § 1 PCPC and art. 187 § 1 ACPC). The resolution of the Polish Supreme Court in extended composition is binding for the case (Art. 398[17]§ 2 PCPC and Art. 187§ 2 ACPC). The Polish Supreme Court or the Polish Supreme Administrative Court in extended composition may take the matter for their recognition (Art. 398 § 3 PCPC 17 and Art. 187 § 2 ACPC).

A similar solution lies in art. 60 of the Act on the Polish Supreme Court. If in the case law of common courts, military courts or the Polish Supreme Court reveal discrepancies in interpretation of the law, the First Chairman of the Supreme Court may submit a request for their decision to the Supreme Court composed of seven judges or other suitable composition (§ 1).

According to § 2, the application referred to in § 1, may also be submitted by Ombudsman and the Attorney General and, within its jurisdiction, the Ombudsman for Children, the Chairman of the Social Dialogue, Chairman of the Financial Supervision Commission and the Ombudsman Financial.

6.5 Application of art. 79 of the Constitution

According to art. 79.1 of the Polish Constitution, anyone whose constitutional freedoms or rights have been violated has the right, under the terms of the Act, to submit the complaint to the Polish Constitutional Tribunal on the constitutionality of a law or other normative act under which a court or organ of public administration has made a final decision on his freedoms or rights or on his obligations specified in the Constitution.

7. Summary

In the above circumstances the issue of ways of information about rights and their impact on the protection of rights in Poland is a very important practical question.

Since the statutory law is understood in divergent could people know uneven manner, which is expressed by divergent court rulings so how the law? How they should shape their goals and plans for a legal sense, since they are not sure about what rights they enjoy and that those granted to them by one law will not be picked up by another law?

In the Polish context one of the major problems for citizens is therefore obtaining information about the law, which affects the possibility of realization of the rights of every citizen. Of course, people with high material status may hire professional lawyers and allocate sufficient money to to assert their rights before the court, however, people with lower financial status must obtain information on the law in a different way.

There is a especially high correlation in Poland between the financial standing of individuals and their possibility of defending their rights. The right to information on law can be fully used only by the people with good financial status. The actions of the government and various non-governmental organizations must aim at creation of such conditions and methods of informing the people on their civil and private rights that enable everyone whose rights have been violated to obtain legal protection regardless whether or not it has sufficient financial resources to initiate proceedings and to take a lawyer.

Information on law also requires the use of language and vocabulary adapted to education and intellectual abilities of the recipient. This is particularly important in Poland, where the process of formulating standards and regulations is very complicated and difficult, causing a problem of interpretation, not only among the addressees of legal norms, but even among professional lawyers.

The Power of Information on the Religion of Others: Marginalization and Alienation of Muslim Students in Greece and the EU

by Konstantinos Kalemis[1, 2, 3]

1. Introduction

The end of the Cold War and the subsequent breakup of the Soviet Union towards the turn of the 20th century led to the dismantling of ideological barriers and divisions and infused a sense of renewed optimism for peace, stability, and development within the international community at large. This optimism was, however, short-lived as the world became witness to the emergence of new kinds of entrenched conflicts and insidious acts of xenophobia and discrimination based on ethnicity. Mass killings and brutal human-rights violations were perpetrated in the Balkans, in which the Muslims were among the most affected victims. The Srebrenica Genocide is one of these unfortunate examples. The situation took a turn for the worse in the aftermath of the 9/11 terrorist attacks in the US. Discrimination and intolerance towards Muslims and defamation of Islam, particularly in Europe and North America, reached alarming and unprecedented proportions. Distortion of the image of Islam and smear campaigns to defame this faith as "*supportive of extremism*" have been on the rise while Muslims were treated with suspicion and in many cases profiled as potential terrorists.

As a result, Muslims became victims of various forms of discrimination, stereotyping, and violation of their human rights. The Muslim world's concern over growing Islamophobia was voiced very strongly by the Heads

1 D.Ed., MA, MSc, M.Ed., Instructor at the National Centre for Public Administration and Local Government in Adult Education & Lifelong Learning.

2 Scientific Associate at the Department of Primary Education in National & Kapodistrian University of Athens.

3 Dept. of Post Graduate Studies in Dept. of Geology and Geoenvironmental in Strategies Management in Natural Disasters in National & Kapodistrian University of Athens, email: kkalemis@primedu.uoa.gr & kkalemi@geol.uoa.gr.

of State and Government and leaders of delegations at the 11th OIC Summit held in Dakar, Senegal, on March 13-14, 2008. In their statements, the leaders condemned the campaign of hatred and intolerance against Islam and discrimination towards Muslims by a marginal group of individuals with vested interests. The 20th Arab Summit held in Damascus on March 29, 2008, underscored that the escalation of the vicious campaign on Islam and the growing phenomenon of Islamophobia and discrimination faced by Muslims in Western societies are matters of deep preoccupation indeed, particularly in view of the defamation and insults of Islam and Muslims in countries that were once known for their pluralism and acceptance of the other.

The current state of unilateralism prevailing in the world calls for a greater effort to close the widening gap between cultures and civilizations. Hence cooperation between the League of Arab States, the OIC, and other relevant organizations is important in order to face up to this phenomenon and the rising grave misperception and discrimination towards Islam, which calls for moderation, tolerance, and acceptance of the other. The relation between religion and politics continues to be an important theme in political and social sciences[4], despite the emergent consensus (both among political theorists and in practical political contexts, such as the United Nations) on the right to freedom of conscience and on the need for some sort of separation between church and state[5]. One reason for the importance of this topic is that religions often make strong claims on people's allegiance[6], and universal religions make these claims on all people, rather than just a particular community. For example, Islam has traditionally held that all people owe obedience to Allah's will. Thus, it is probably inevitable that religious commitments will sometimes come into conflict with the demands of politics. But religious beliefs and practices also potentially support politics[7] in many ways.

4 Kymlicka, Will. *Multicultural Citizenship: A Liberal Theory of Minority Right.* Oxford: Oxford University Press, 1995.

5 Audi, Robert, and Nicholas Wolterstorff. *Religion in the Public Square: The Place of Religious Reasons in Political Debate*. Lanham, MD: Rowman & Littlefield, 1997.

6 Burtt, Shelley, "Religious Parents, Secular Schools: A Liberal Defense of Illiberal Education", *The Review of Politics* 56.1 (1994): 51-70.

7 Clanton, J. Caleb. *Religion and Democratic Citizenship: Inquiry and Conviction in the*

The extent and form of this support is as important to political philosophers as is the possibility for conflict. Moreover, there has been a growing interest in minority groups and the political rights and entitlements they are due. One result of this interest is substantial attention given to the particular concerns and needs of minority groups who are distinguished by their religion, as opposed to ethnicity, gender or wealth.

1.1 Establishment and separation of Church and State

While the topic of establishment has receded in importance at present, it has been central to political thought in the West since at least the days of Constantine. The term "establishment" can refer to any of several possible arrangements for a religion in a society's political life. These arrangements include – among the others - the following:

1. A religious body may be a "state" church[8] in the sense that it has an exclusive right to practice its faith.
2. Particular ecclesiastical officials may have, in virtue of their office, an established role in political institutions[9].
3. A church may simply have a privileged role in certain public, political ceremonies (for example, inaugurations, opening of parliament, etc.).
4. Instead of privileging a particular religious group, a state could simply enshrine a particular creed or belief system as its official religion, much like the "official bird" or "official flower."

Even today, there are strains of conservatism that argue for establishment by emphasizing the benefits that will accrue to the political system or society at large (Scruton, 1980). According to this line of thought, the healthy *polis* requires a substantial amount of pre- or extra-political social cohesion. More specifically, a certain amount of social cohesion is necessary both to ensure that citizens see themselves as sufficiently connected to each other

American Public Square. Lanham, MD: Lexington Books, 2007.

8 Eliot, T. S. "Catholicism and International Order." *Essays, Ancient and Modern.* London: Faber and Faber, 1936.

9 Gaus, Gerald F. "The Place of Religious Belief in Liberal Politics." In *Multiculturalism and Moral Conflict*, edited by Maria Dimova-Cookson. London: Routledge, 2008.

(so that they will want to cooperate politically), and to ensure that they have a common framework within which they can make coherent collective political decisions. This cohesion in turn is dependent on a substantial amount of cultural homogeneity, especially with respect to adherence to certain values. One way of ensuring this kind of homogeneity is to enact one of the forms of establishment mentioned above, such as displaying religious symbols in political buildings and monuments, or by including references to a particular religion in political ceremonies.

Against these positions, the liberal tradition has generally opposed establishment in all of the above forms. Contemporary liberals typically appeal to the value of fairness. It is claimed, for example, that the state should remain neutral among religions because it is unfair-especially for a democratic government that is supposed to represent all of the people composing its demos-to intentionally disadvantage (or unequally favor) any group of citizens in their pursuit of the good as they understand it, religious or otherwise (Rawls, 1971).

Similarly, liberals often argue that fairness precludes devoting tax revenues to religious groups because doing so amounts to forcing non-believers to subsidize religions that they reject. A different approach for liberals10 is to appeal directly to the right to practice one's religion, which is derivable from a more general right to freedom of conscience. If all people have such a right, then it is morally wrong for the state to force them to participate in religious practices and institutions that they would otherwise oppose, such as forcing them to take part in public prayer. It is also wrong, for the same reason, to force people to support financially (via taxation) religious institutions and communities that they would not otherwise wish to support.

2. Definitions

The word "marginalize" means to put or keep (someone) in a powerless or unimportant position within a society or group. As a second meaning, marginalize means to relegate to an unimportant or powerless position within a society or group. The word "alienation" has more meanings, like:

10 Larmore, Charles. *Patterns of Moral Complexity*. Cambridge: Cambridge University Press, 1987.

(1) the act of alienating or the condition of being alienated; estrangement, (2) emotional isolation or dissociation[11]. So far, in the situation of immigrants, the means focus on the state of being an outsider or the feeling of being isolated, as from the rest of the society. The dictionary definition of the word "phobia" is "*a strong fear or dislike: an irrational or very powerful fear and dislike of something*". Simplistic as may be, Islamophobia by this very definition would mean an irrational or very powerful fear or dislike of Islam and the feeling as if the Muslims are under siege and attack. Islamophobia however goes much beyond this and incorporates racial hatred, intolerance, prejudice, discrimination and stereotyping.

The phenomenon of Islamophobia in its essence is a religion-based resentment. It has two distinct aspects: (1) from the viewpoint of the protagonists of Islamophobia and (2) from the victims' point of view. Islamophobia is a much used but little understood term. Although there is currently no legally agreed definition of Islamophobia, nor has social science developed a common definition, policy and action to combat it is undertaken within the broad concepts of racism and racial discrimination, which are universally accepted by Governments and international organizations. The EUMC therefore bases its approach to identifying the phenomenon and its manifestations on internationally agreed standards on racism and the ongoing work of the Council of Europe and United Nations.

A distinction must also be made between attitudes and actions against Muslims based on unjust stereotypes and criticism of Muslim beliefs that can be seen as undermining fundamental rights. The common fundamental principles of the European Union[12] and its Member States under Community law, the Charter of Fundamental Rights of the European Union and the European Convention for Protection of Human Rights and Fundamental Freedoms, must be respected.

These values include respect for the uniqueness and freedom of the individual, freedom of expression, equal opportunities for men and women (including the equal right of women to make individual choices in all

11 The American Heritage Dictionary of the English Language, 5th Edition. 2011 by Houghton Mifflin Harcourt Publishing Company. Published by Houghton Mifflin Harcourt Publishing Company.

12 Rawls, John. "The Idea of Public Reason Revisited." *The Law of Peoples.* Cambridge, MA: Harvard University Press, 1999.

areas of life) and equal treatment and non-discrimination on a number of grounds, including, for example, sexual orientation. Efforts to protect those principles may at times clash with the perceptions of religious duties of certain individuals or faith groups[13]. However, this perspective is of fundamental importance and Member States have a positive duty under international human rights law to protect and promote these values, while ensuring that a potential critical stance towards certain attitudes of other groups in society respects the principle of equal treatment[14].

2.1 Marginalization and alienation

The central question to be considered is whether Muslims feel integrated in European societies, or whether sections of Muslim communities and individuals experience social exclusion, marginalization and alienation. Such a consideration is central to the role of the EUMC, where the overall focus of our work is on vulnerable groups who are victims of racism and discrimination. The marginalization and alienation of individuals or groups from society is a central issue for the EUMC. In addition to thematic reports on the situation of migrants and minorities in the areas of employment, housing and education in the EU, the EUMC has also conducted pilot 'discrimination studies' on migrants' experiences of racism and xenophobia in different areas of economic and social life. These pilot studies were conducted in several European countries between 2002 and 2005 among selected migrant groups using a range of sampling techniques and methodologies. Although the results are not directly comparable, they provide useful background information that is able to inform on the experiences of selected migrant groups and, in some countries, the experiences of Muslim groups.

The disadvantaged position of Muslim minorities, evidence of a rise in Islamophobia and concern over processes of alienation and radicalization have triggered an intense debate in the European Union regarding the need for re-examining community cohesion and integration policies. A series

13 Rorty, Richard. "Religion as Conversation-stopper." *Philosophy and Social Hope*. New York: Penguin Putnam, Inc., 1999.

14 Sandel, Michael J. *Liberalism and the Limits of Justice*. Rev. ed. Cambridge: Cambridge University Press, 1998.

of events such as the September 11 terrorist attacks against the US, the murder of Theo van Gogh in the Netherlands, the Madrid and London bombings and the debate on the Prophet Mohammed cartoons have given further prominence to the situation of Muslim communities. The central question is how to avoid stereotypical generalizations, how to reduce fear and how to strengthen cohesion in our diverse European societies while countering marginalization and discrimination on the basis of race, ethnicity, religion or belief. European Muslims are a highly diverse mix of ethnicities, religious affiliation, philosophical beliefs, political persuasion, secular tendencies, languages and cultural traditions, constituting the second largest religious group of Europe's multi-faith society.

In fact Muslim communities are no different from other communities in their complexity. Discrimination against Muslims can be attributed to Islamophobic attitudes, as much as to racist and xenophobic resentments, as these elements are in many cases inextricably intertwined.

3. The multi-cultural education: differentiation as effective instruction

The diversity of the 21st-century classroom creates numerous challenges for teachers who may not have known the same diversity themselves as students. Among these, teachers must balance the requirements of high-stakes accountability while meeting the needs of diverse students within their classroom. The 26th Annual Report to Congress on IDEA reported that approximately ninety-six percent of general education teachers have students in their classroom with learning disabilities. This is not a surprising statistic, considering there are over six million students with disability classifications in the United States. The frequency of special education students in the classroom, however, is only one of the obstacles that teachers face. Teachers must also contend with an increasing number of students from culturally and linguistically diverse backgrounds and from high-poverty families.

By contrast[15], the practice of differentiating instruction helps teachers

15 Eliot, T. S. "The Idea of a Christian Society" and "Notes Toward the Definition of Culture." *Christianity and Culture.* New York: Harcourt Brace & Company, 1967.

address rigorous standards while responding to the individual needs of students. Differentiation allows teachers to focus on essential skills in each content area, be responsive to individual differences, incorporate assessment into instruction, and provide students with multiple avenues to learning. The result is a classroom where specialized instruction is the norm for all students. Students with disabilities have access to appropriate modifications, while students who excel have access to appropriate challenges. This model for instructional planning and delivery is not a new idea and is widely touted as the most promising solution to many of the obstacles presented by the proliferation of diverse classrooms.

The pressures of classroom management[16] needs can also be alleviated as a result of using technology to differentiate instruction. Classrooms enhanced by technology provide support and structure to students who need scaffolding and enrichment to students who thrive on challenge.

The result is a learning environment that is task-centered and predictable, in which students understand what's expected of them and how to succeed. In a classroom where gifted learners, learners with learning disabilities, and learners with other special needs are all challenged at appropriate levels at the same time, students are more likely to be engaged in learning activities and less likely to be engaged in inappropriate behaviors. In such environments, classroom management works differently: Teachers act more as facilitators, which allows for more individual attention to students who need attention and might otherwise behave inappropriately as a result.

Muslim pupils have been present in the educational systems of several Member States[17], such as Belgium, France, Germany, Austria, Sweden, the Netherlands and the United Kingdom for some time. On the other hand, in Member States such as Greece, Italy, Spain, Portugal, Finland, Ireland, and, to some extent, Denmark, the Muslim pupil population has only recently began growing, as immigration reached these countries much later. Due to the lack of educational statistics based on religion or ethnicity an assess-

16 Kymlicka, Will. *Contemporary Political Philosophy: An Introduction*. Oxford: Oxford University Press, 2002.

17 MacIntyre, Alasdair. *After Virtue: A Study in Moral Theory*. 2nd ed. Notre Dame, IN: University of Notre Dame Press, 1984.

ment of the educational situation of Muslim pupils can be inferred mainly indirectly by looking at data referring to nationality or country of origin. These do not reveal the effects of a complex array of other factors contributing to school performance and educational attainment. The results of the 2000 and 2003 OECD PISA studies and the 2006 OECD report on migrant student performance show that non-native born pupils have much lower literacy scores than native pupils.

Particularly in countries where the educational and socio-economic status of migrant families – many with Muslim background – is comparatively low, the performance gaps between students with and without migrant backgrounds tends to be larger. The 2006 study suggested that although students with migrant origins generally have strong learning dispositions, the performance differences between native and such students are significant, particularly in Austria, Belgium, Denmark, France, Germany and the Netherlands.

4. Methodology

The sample consisted of 167 German-Arabs, 184 Arab-Turks and 205 British-Pakistanis. Most of the participants were young adults and the three groups did not differ in terms of age. There were more female participants among the German-Arabs and Arab-Turks than in the British-Pakistani sample. However, each sample could be described as relatively even in terms of gender distribution. While nearly halfofthe German-Arab participants were second generation immigrants,this applied to more than two thirds of the Arab-Turks and only to about one fourth of the British-Pakistanis.

The British participants reported a better education than their German counterparts. Nearly two-thirds of the British-Pakistanis, but only 37.6% of the Arab-Turks and 23.6% of the German-Arabs held a university degree. German-Arabs and Arab-Turks reported mostly primary or secondary school as their highest education. Procedure Data was collected through online surveys between the period of January and February 2015.

The surveys were translated from English into German and French using forward-back translation by bilingual teams. Participants were recruited through Muslim organizations, Muslim online newspapers, personal contacts and social networks. Before participating, respondents were in-

formed about the study's purpose, its confidentiality and the right to withdraw from participation at any given time.

Muslims are inadequately captured in demographic statistics: the most conservative estimate based on official and, where they are not available, unofficial data is of a Muslim population of around thirteen million, around 3.5 per cent of the total population of the European Union, but with great variations between Member States. The demographic profile of the Muslim population is reportedly younger than the general population, indicating that policy interventions aimed at young people should have a strong impact.

In Greece there are no positive measures to facilitate religious activities of minority groups at the workplace. The NGO Migrants' Forum during the past years has asked for the recognition of Muslim festivities as grounds for legitimate absence from work.

The provision of Islamic religious education varies across Europe, ranging from formal secular religious education – which is multi-faith in nature – to cross curriculum teaching of Islam, and separate Islamic teaching provided within or outside the state school context. Aspects of Islam are also taught within history curricula and, to a lesser extent, Islamic themes are also covered in some language and literature curricula.

5. Results

Muslims in the Member States of the European Union experience various levels of discrimination and marginalization in employment, education and housing, and are also the victims of negative stereotyping by majority populations and the media. In addition, they are vulnerable to manifestations of prejudice and hatred in the form of anything from verbal threats through to physical attacks on people and property. Discrimination against Muslims can be attributed to Islamophobic attitudes, as much as to racist and xenophobic resentment, as these elements are in many cases inextricably intertwined. Racism, xenophobia and Islamophobia become mutually reinforcing phenomena and hostility against Muslims should also be seen in the context of a more general climate of hostility towards migrants and minorities.

The findings of this report had been gathered as information from all

EU Member States with widely different histories of, and responses to, issues related to religious diversity, and very different traditions of anti-racism and anti-discrimination awareness and activity. Despite the variety in the nature of the data and information collected, it is evident that Muslims often experience various levels of discrimination and marginalization in employment, education and housing, and are also victims of negative stereotyping and prejudicial attitudes. It is difficult to attribute such discriminatory phenomena exclusively to religion, as Muslims are likely to become victims of multiple discrimination on the basis of their religion, race, national or ethnic origin, language, color, nationality, gender, and even legal status.

This report finds that Muslims are vulnerable to discrimination and manifestations of Islamophobia in the form of anything from verbal threats through to physical attacks on people and property. The report presents research and statistical data – mostly through 'proxy' data, referring to nationality and ethnicity – showing that Muslims are often resident in areas with poor housing conditions, while their educational achievement generally falls below national averages and their unemployment rates tend to be higher than average. Muslims tend to be employed in jobs that require lower qualifications and as a group they are over-represented in low-paying sectors of the economy. Thus, many Muslims, particularly young people, face limited opportunities for social advancement and experience social exclusion and discrimination. Yet, given the paucity of available data, it is clear that the true extent and nature of discrimination and Islamophobic incidents against Muslims continues to be under-documented.

Other important areas are:

- Cultural events are an excellent way of introducing Islam to non-Muslims and can easily build upon any existent interest that might be identified. Such events are also easily transferable to other national settings where good ideas from one member state can be used elsewhere.
- Awareness programs are another means by which these same objectives can be achieved, where a range of organization can become involved. A number of excellent examples were identified, including in Ireland where the issue of Islamophobia is being incorporated into a national anti-racism programme, entitled «Know Racism».
- Interaction and co-operation between the media and Muslim or-

ganizations must also be established. One recommendation might be to reflect the way in which the Dutch media are openly working in conjunction with both the Muslim community and interested researchers to assess the impact of Islamophobia in the media.

The problem of social marginalization must be tackled and the practice of segregation must be addressed. Where such groups continue to retreat and become ever more introverted they no longer identify themselves with either a local, national or even European identity.

6. Scope of analysis: Muslims in Greece and Europe

Muslims in Europe have been facing even greater discrimination than Muslim Americans in civic and political life, as hinted above. Despite the stated EU major objectives of its recent Racial Equality Directive with regard to citizenship and integration for Muslim and other minorities and communities, and despite the fact that "by the end of 2006, legislation transposing the Racial Equality Directive had been adopted", the EU Agency for Fundamental Rights, recognizes that "in the thematic areas of legal issues, employment, housing, education, and racist violence and crime (…), in many [EU] countries there is no indication that a single sanction had been applied or compensation awarded in cases of ethnic discrimination during 2006". This is being the case, even though "regular evidence" exists that shows "ethnic discrimination", "gross exploitation", "exclusion", and "inequalities", in all the above-listed areas, in addition to "neglect of mother tongue education" and "racist violence and crime […] across the EU". More importantly, despite its recommendations of good practices, the FRA 2007 Report (p. 14), furthermore and more importantly, notes that "there continue to be disturbing reports of violence and malpractice against vulnerable minorities by agents of the state—police, immigration, and border control personnel—in many [EU] countries". Consequently, since European Muslims tended to be much less socio-economically integrated than Muslim Americans, their feelings of alienation have been correspondingly higher. Thus, Muslims in Europe have faced even greater discrimination than Muslim Americans in civic and political life and have encountered several barriers to integration. The ethnic and religious diversity that has long been a fact of American life is a relatively new phenomenon in most

Western European nations.

Interest in citizenship education and diversity has also developed in response to a growing awareness of the importance of learning to live together not only in nations characterized by diversity, but also in local communities and a global community characterized by diversity. Educators have increasingly given attention to intercultural skills and to the concepts of cosmopolitan and global citizenship in an effort to address diversity at different scales from the local to the global. International organizations such as UNESCO and the Council of Europe have given attention to the global and regional (European) dimensions of citizenship education, exploring ways in which learners might be encouraged to exercise concern and loyalty towards fellow humanity beyond the borders of the nation-state. These developments raise particular challenges for education policy-makers and curriculum planners, as pressures to address questions relating to unequal power-relations both within communities and nation-states, as well as in international relations, have come to the fore.

6.1 Citizenship education and the nation-state

Citizenship education[18] which encourages or demands loyalty to the nation can be traced back to the late nineteenth century and to the development of mass education. Indeed, John Dewey has observed how in Europe the development of mass publicly-funded schooling[19] occurred at a time when nationalism was at its zenith, so that public schooling itself became part of the nationalist project. The exclusive nationalism promoted across the curriculum, and specifically through subjects such as history and civics, not only replaced an earlier tradition of cosmopolitanism, or loyalty to fellow humanity, but also stressed national homogeneity by denying or ignoring ethnic and linguistic diversity within the nation, and asserting that specific inequalities, such as those relating to class, gender and race, were part of a natural social hierarchy, divinely ordained.Such fictions were upheld in

18 Brighouse, Harry. *School Choice and Social Justice.* Oxford: Oxford University Press, 2003

19 Callan, Eomann, *Creating Citizens: Political Education and Liberal Democracy*. Oxford: Clarendon Press, 1997.

schooling and through the curriculum throughout the early twentieth century, although they were challenged, both by pacifists after World War One and also by the developing anti-colonial struggles of this era. In the second half of the twentieth century, the struggles of anti-colonial, civil rights and feminist movements effectively pressed for changes to school curricula.

These movements also raised public awareness of the ways in which traditional approaches to the education of citizens distinguished between learners from different social class background[20]. The citizenship education of established elites continues to prepare them for leadership roles, whereas the masses often continue to learn that their role is, at best, to vote for their leaders, and then accept their authority.

7. Globalization, migration and citizenship

At the beginning of the twenty-first century, nations-states across the globe are experiencing new challenges as the forces of globalization[21], new and intensifying international migration, and the activities of transnational communities and corporations, promote increased cross-border movements and networks. The diverse citizenship status of students poses additional challenges to educators, not least in contexts where the curriculum assumes that all learners are nationals of the country in which they are studying. Formal education policy and curricula rarely acknowledge these forms of diversity in the citizenship education classroom. Citizenship education carries the duty of enabling the young to develop their social and political identities; acquire the skills to become active participants in society; and engage with others on the basis of respect.

These tasks are made more complex in contexts of growing international migration[22]. Immigration raises two broad types of question for citizenship educators. The first relates to the need to respond to growing cultural diversity in schools and schools' mission of assuring equality of opportu-

20 Gutmann, Amy. *Democratic Education.* Rev. ed. Princeton, NJ: Princeton University Press, 1999.

21 Okin, Susan Moller (eds.), *Is Multiculturalism Bad for Women?,* Joshua Cohen, Matthew Howard, and Martha C. Nussbaum. Princeton, NJ: Princeton University Press, 1999.

22 Rorty, Richard. *Contingency, Irony, and Solidarity.* Cambridge: Cambridge University Press, 1989.

nity for all. This is a considerable challenge in the context of asymmetrical power relations between established citizens and newcomers. The second relates to the role of education in general and citizenship education in particular in forming and extending the various social and political identities of learners and equipping them with the tools they need to become engaged members of their communities. In other words, schools are tasked with role of supporting young people, both migrants and established citizens, to become actively engaged in their communities, regardless of their formal citizenship status and with the task of ensuring that newcomers integrate.

In reality these two tasks are clearly inter-related, for unequal access to educational and employment opportunities (experiencing exclusion and discrimination), not only undermines the everyday work of citizenship educators, but may adversely affect learners' readiness to participate, raising an additional barrier in enabling them to become active citizens. Nation-states, in enacting education and wider social policies, often assume that integration is a one way process, failing to anticipate that newcomers are likely to impact on the majority culture or contribute to a broader process of social or cultural transformation. Efforts by the nation-state to manage or control this process, particularly where assumptions are made about the temporary presence of workers, mean that little or no attention is given to the social needs of families, including the education of children. Consequently, citizenship education programs are at best inappropriate, and risk alienating learners and undermining the processes of social cohesion they purport to strengthen. In such contexts ethno-cultural diversity may be seen by elites as a threat to the future stability of the nation.

This, in turn, may be a self-fulfilling prophecy, if the social rights and in particular the educational rights of young people are neglected. The denial of such social rights as equal access to education can in itself lead to social conflicts, so undermining social stability.

8. Council of Europe Charter on Education for Democratic Citizenship and Human Rights Education

The Council of Europe Charter on Education for Democratic Citizenship and Human Rights Education, adopted by Recommendation CM/Rec (2010)7 of the Committee of Ministers of the member states of the Council

of Europe is significant to those concerned with citizenship education in contexts of diversity in a number of respects. First, this represents a key step by an international organization to establish normative standards on citizenship education which transcend national boundaries. Second, in seeking a common framework for education for democratic citizenship across the 47 member states of the Council of Europe, based on universal human rights(rather than exclusive citizenship rights), it exemplifies an alternative concept of citizenship education in which the status of citizenship status is judged to be secondary to the need to promote a feeling of citizenship and engaged acts of citizenship. Finally, the model represented by the Council of Europe Charter is potentially a challenge to the dominant nationalist model of citizenship education. Each of these features is relevant to the question of diversity, since a conception of citizenship education which relies on the assumption that all learners have citizenship status is problematic, as discussed above. Nevertheless, the actions required by learners to engage fully in citizenship learning require them to demonstrate solidarity with others rather than to engage in any direct or personal struggle for rights. There is little, if any, recognition that the realization of justice and equality may require learners to engage in struggle or conflict. In this sense this model seems to assume the leaner belongs to a privileged majority rather than to any disadvantaged group vulnerable to discrimination.

The model fails to engage fully with the historical reality that demonstrates that human rights have rarely, if ever, been conceded by the powerful to the powerless, without a struggle.

9. Multicultural citizenship and intercultural learning

In an article discussing multicultural states and intercultural citizens, Will Kymlicka raises some central dilemmas relating to citizenship education policies in contexts of diversity. He interrogates the image of the state and questions what changes need to take place to enable or realize a genuinely multicultural state. He asks the reader to imagine what it would mean for the state to change so that the constitution, institutions and the laws of the state were multicultural. He then develops his argument to focus on the citizens of a genuine multicultural state. Citizenship generally refers to membership of a political community and therefore implies a relationship between the individual and the state. What qualities does the multicultural

state require of individual citizen? Kymlicka draws on the concept of interculturalism to discuss the types of knowledge, beliefs, virtues and dispositions that an intercultural citizen would possess. Ideally, the multicultural state needs its citizens to engage with each other and with teh apparatus and institutions of the state so as to enable and sustain the state and create a workable interaction between citizens. In other words, there needs to be a good fit between the model of the multicultural state and the competencies of intercultural citizen. Kymlicka identifies a number of tensions between promoting desirable forms of multiculturalism within state institutions and promoting desired forms of interculturalism within individual citizens.

Education plays a key role in enabling this good fit. Unfortunately, it can also work to upset the balance between creating a just society based on multicultural ideals, by focusing too strongly on the interactions between citizens, and failing to expose the unequal systems of a state which is a de facto multicultural society (by nature of its diverse population). Some proposals to promote increased intercultural skills and knowledge within individual citizens ((that is efforts to address diversity within citizenship education) are enacted precisely to avoid greater institutional changes within the state.

Schools, alongside other state institutions, have a key role in preparing for equal citizenship in a multicultural state. Schools and other public institutions have as a central aspect of their mission, the key role of challenging discrimination, working to accommodate diversity, promote integration, and to enable all learners to imagine a more inclusive image of the nation. In a very real sense, citizenship education policies and practices need to be enacted within a set of broader social, economic and political policies and legal frameworks which reinforce, rather than undermine, the position of minorities and historically disadvantaged groups.

10. Conclusions

Muslims in the Member States of the European Union experience various levels of discrimination and marginalization in employment, education and housing, and are also the victims of negative stereotyping by majority populations and the media. In addition, they are vulnerable to manifestations of prejudice and hatred in the form of anything from verbal threats through to physical attacks on people and property. Discrimination against Muslims can be attributed to Islamophobic attitudes, as much as to racist

and xenophobic resentment, as these elements are in many cases inextricably intertwined. Racism, xenophobia and Islamophobia become mutually reinforcing phenomena and hostility against Muslims should also be seen in the context of a more general climate of hostility towards migrants and minorities. Yet, given this situation, the true extent and nature of discrimination and Islamophobic incidents against Muslim communities remains severely underreported and under-documented in the EU.

There is a serious lack of data or official information on, first, the social situation of Muslims in Member States and, second, on the extent and nature of Islamophobic incidents.As a reflection of this, policy makers are not well informed at both national and EU level about the specific situation of Muslims in the areas of employment, education and housing, as well as about the extent and nature of discrimination, incidents and threats targeted at Muslims.

The Role of private radio station in promoting free debate in Lesotho

Mamolise Martha Falatsa

1. Introduction

Theoretical framework

This paper is formed by the participatory theoretical framework because it is investigating the role of private radio played by radio stations in providing audience participation. Participatory communication is the theory and practices of communication used to involve people in the decision making process. Participatory communication encourages participation stimulating critical thinking and stresses the process of participation.

The role of media refers to the purposes or service that media provide to the society (Ugangu2012:1).Christian; Glasser; Mc Quail; Nordenstreng & White (2009) succinctly puts that the important roles of media are monitorial, facilitative, radical and collaborative functions. According Christian et.al (2009) the monitorial role refers to the case where the media seeing themselves as neutral observers reporting objectively about the world; whilst in facilitative role media are distanced from the centers of power and seek to provide citizens with a platform for expressing their views and participate in the political processes. The radical role of media refers to a totally oppositional approach to the prevailing power. Lastly is the collaborative role that refers to the case where media directly serves the government and other centers of power.

Whilst Ugangu(2012:53) asserts that the African independence leaders did not consider media as the watchdogs because this role secures individual based rights such as freedom of expression and right to participate in civic processes. According to Ugangu (2012) the role of media were highly correlated with the attitudes and goals of the high government officials. This situation continued until the age of liberation in the early 1990s.

Furthermore, Ugangu(2012:53) asserts that the elites ensure that the ordinary people's voice were shut out of national debates as such the political

elites became the main subjects for the news, while issues affecting people's life were relegated on media news agenda. According to Ugangu this group realized that media was a good tool to keep them in power.

Worldwide radio plays a pivotal role in relaying information from sources to the recipients, and in most of African countries radio is the most popularly and largely accessed media platform. Ugangu (2012:2) affirms this by pointing that FM radio continues to be chief initiator of powerful medium of debate in Kenya. Ricardo points out that in Mozambique in order to reach the majority of the citizens radio and television are the main communication platforms in the communication (Ricardo 2015:3).

According to Ugangu FM radio stations are emerging as influential agents shaping perceptions towards socio-economic and political transformation of the society. Ugangu (2012: 53) asserts that the growth and expansion of media has generally provided and made possible for ordinary people to access many sources of information. According to Ugangu(2012) expansion of media has created possibilities to the ordinary people to participate in national and global information irrespective of the traditional limitations associate with literacy and class distinction.

2. Background of the study

Lesotho has been has been governed in many different ways since its founding as a nation in the mid-19th century, including episodes of democratic authoritarian regimes. Kapa (2013:15) posits that 1993 marks return of Lesotho to multi-party politics from about 22 years of undemocratic rule being ruled by authoritarian Basotho National Party from 1970 to 1986 and Military from 1986 to 1993. According to Kapa this period also marks a period of extreme secretive rule, that prohibited public participation in policies making, and characterised by prohibition of public servants release of information to the public without authorisation by the respective heads of ministries and principal secretaries which can also be explained in terms of absence of law and policy of receipt and access of information (Kapa 2013:15).

This period marks changes in social, economic and political development and move of the country. In 1999 Lesotho liberalised communication and allowed increasing public and media freedom of expression. Metsing

in 2007 while officially opening a workshop on communication issues in Southern Africa pointed out that, the landscape of Lesotho broadcasting sector has changed quite significantly and the situation moved from where airwaves were dominated by Radio Lesotho, and there is diversity in the ownership and running of broadcast media sector with private stations licensed (Metsing 2007:1).

According to Metsing(2007), the broadcasting media play a crucial role in shaping most people's lives, due to their daily reliance on them for news and information that shape their views and perceptions on political, economic and social issues (Metsing 2007:1). MISA Lesotho (20013:49) posits that Lesotho radio programmes are characterised by vibrant listener participation.

MISA Lesotho (2013:49)**,** provides that there are about fourteen radio stations on air and freedom of speech is evident as the people call in throughout the day and night to air their views on any topic without fear. However MISA (2015:34) reports that, most of the radio stations both government and privately owned and television jammed on the 30 August 2014. According to MISA, Lesotho radio stations have traditionally been a valuable source of information for citizens and a vibrant forum for discussion and citizen participation through the phone- in facilities, however with the political instability, which has been growing since 2013 are no longer free.

Kapa (2013:15) points out that, since 1993 Lesotho have witnessed a growing number of private and community media institutions both print and electronic. To add on UNESCO (2009:1) reports that the Government of Lesotho issued broadcasting licences to private radio stations mostly based in Maseru.

There emerged the following radio stations in broadcast in frequent modulation(FM) and covers city of Maseru Moafrika FM; Catholic (CR) FM; Joy FM; People's Choice (PC) FM; Harvest FM; Thaha Khube (TK) FM; Kereke ea Evangelic Lesotho (KEL) FM and Jesu ke Karabo (JKK) FM; Department of Physics and Electronics (DOPE) FM owned by National University of Lesotho (NUL) co- existed with the two national radio stations, namely, Radio Lesotho and Ultimate FM (Matjama 2007: 3). However currently Lesotho has about fifteen radio stations with about three newly established genre of community radio stations with the assistance of

UNESCOM Lesotho namely Motjoli Community FM ; Moeling community FM; Mafeteng Community FM and three other private owned radio stations Molisa ea Molemo FM ;T`senolo FM and Sublime FM.

According to Kapa this is a positive development as it provides citizens with avenues for exercising their freedom of expression rights and allows them to participate in national issues. Kapa adds that, citizens of Lesotho have enjoyed high degree of freedom of speech including criticizing their governments freely. Although observes that there still remains a challenge of state owned broadcast media which enjoy wider national coverage which remain firmly under government control. In this media government dictates what should be broadcast and who should access these institutions for the purpose of expressing views and disseminating information.

Although the Lesotho airwaves were liberalised 1999, but Matjama (2007:3) argues that the regulatory environment is nonetheless deficient because the broadcasting regulatory body, Lesotho Communication Authority (LCA), is still subjected to the authority of the Minister of Communication, Science and Technology. He further indicates that the Act which established the LCA has been partially implemented, and this resulted into the non-adoption of a media policy in Lesotho and further asserts that this is one of the factors contributing to the hostility of the media environment.

As such Matjama (2007:3) and MISA (2013:47) alleges that both the Media Policy and the Receipt and Access to Information Bill have been gathering dust in parliament shelves since 2000 and thus have not contributed to improving media freedom in Lesotho. According to Matjama (2007:3), Harvest FM was threatened with closure in 2007 after lambasting government policies and governance style.

As such the environment in which media operates in Lesotho is still understood as hostile for democratic debate. MISA (2013:47) contends that media in Lesotho also functions in a very hostile legal environment, because some old laws unfavourable to media freedom and freedom of expression are still valid, such as "the Sedition Proclamation of 1938(No. 44 of 1938) which provides for suppression of sedition and seditious publications and for the punishment of seditious offences, and the Criminal Procedures and Evidence Act of 1981 (No.9 of 1981) which consolidates and amends the law relating to procedure and evidence in criminal cases. "For instance, on the 17th August 2011, four privately owned commercial

radio stations went off air because they had provided a live coverage to the protest embarked on by factory workers(MISA/IFEX 2011:1). MISA/IFEX 2011:1) report that the interruption started less than 24 hours after the meeting between privately owned radio station managers, the Acting Principal Secretary of the Ministry of Communications and Chief Executive of the Lesotho Communications Authority.

Although the is that Lesotho liberalised the airwaves, that led to boom of the privately owned and community radio stations the legal environment in which the they operate in continues to be hostile for them to perform the normative roles discussed by Christian and others. As such it is imperative to conduct a qualitative research to investigate the role of the privately owned radio stations and the facebook pages in promoting free debate.

3. Media Freedom and Civil Liberties Status in Lesotho

The constitution of Lesotho enshrines the right to freedom of expression. African Media Barometer (2010:5) argues that the constitution of Lesotho does not explicitly mention media freedom but allows citizens the right to express and to obtain and impart information. According to African Media Barometer, this clause guarantees these rights only as long as they do not interfere with defence, public safety, morality and health. However, MISA (2013:47) states that despite having held its first ever democratic election in1993 and witnessing the growth of private broadcast media, Lesotho still has no express guarantees for media freedom and freedom of expression.

Even though the government of Lesotho generally respects freedom of speech, has declined in the rankings of the Freedom House, because the Lesotho Communication Authority LCA has increased broadcasting license fee seven folds, from $400 to $3000 and this infringes on the number of the role players, drawing objections from press freedom advocates (Puddington, Piano, Eiss, Neubauer and Roylance 2009:416).

A Freedom House Report (2011:388) outlines that the critical media outlets and journalists in Lesotho face heavy libel charges and are occasionally harassed or attacked. For example, in October 2010, the ABC leader Tom Thabane threatened to shoot a Sunday Express reporter Mr Tlali Caswell for enquiring about members of his family who were facing rape and assault charges lodged by his former wife.

The Country Report on Human Rights Practices (2008:326) points out that on July 18, 2008, an independent radio station, Harvest FM, closed for three days due to a suspension order by the Lesotho Communications Authority (LCA), a regulatory body. According to the Country Report on Human Rights Practices (2008:326), the LCA reportedly received complaints from the Commissioner of Police that the station made inaccurate statements, and complaints from the Principal Secretary of Communications Science and Technology that the station had incited persons to resist the removal of street vendors in the downtown areas of Maseru.

Freedom House (2011:388) reports that independent newspapers and radio stations in Lesotho routinely criticise the government, while the state-owned outlets tend to reflect the views of the ruling party. While the International Monetary Fund (IMF) (2012:388) purports that radio is still the dominant platform for the public debate, incidents such as those cited above suggest that limitations to media freedom are imposed by the state from time to time.

4. The state of the media in Lesotho

The broadcasting sector is growing, particularly in numbers of commercial, private and community radio stations operating. The community radio stations emerged through the assistance of UNESCO to afford rural communities avenues to express their view and participate in national issues such as policy making and community development processes.

There are a variety of media outlets operating in Lesotho, both public and private. These include the emerging number of community radio stations explored in this study. The Commonwealth Secretariat (2012:16) posits that since the government of Lesotho opened up the media sector in 1999 to the independent media sector, this led to growth in the private media, particularly radio stations; while the state's electronic media nonetheless continue to dominate news coverage in all areas of the country. Radio Lesotho, run by the state, covers the entire country, while the majority of private radio stations cover only the densely populated, lower-lying area of Maseru and its periphery.

The state controls the country's largest radio stations and its only television channel, as well as Radio Lesotho, Ultimate FM and Lesotho Television (Commonwealth Secretariat 2012:16). Radio Lesotho and Lesotho

Television have remained Department of Broadcasting services and are run directly by government; existing solely for the dissemination of the government viewpoint and propaganda, and in the process, effectively favouring its rule over other parties (Matjama 2007:3). According to Matjama, the government of Lesotho has shown persistent reluctance in transforming these radio and television outlets into public broadcasters.

In many areas, thus, media freedom in Lesotho was constrained by the government influence and ownership. The International Monetary Fund Report (2012:388) posited that the key challenge of media in Lesotho lies in the state's delays in adopting and implementing a media policy, which would result in the establishment of the relevant institutional infrastructure and legal framework to systematically address issues related to professionalism, ethics, conduct and improvement of media content, as well as coverage. For example, the Freedom House (2011:388) states that in September 2010, the cabinet refused to send the delayed media policy to parliament for approval, and instead returned the policy to the Ministry of Communications.

MISA (2015:31) posited that Lesotho's media freedom was on shaky ground in 2014 as the country suffered extreme political unrest resulted into flee of the former Prime Minister Thomas Thabane to South Africa at the 30th August 2014. According to MISA the former Premier fled the capital Maseru just before the army commander Lieutenant-General Tlali Kamoli attacked his official residence and military units surrounded police stations buildings.

MISA further contended that in this environment they saw no progress towards much needed legal reforms to depoliticise state- owned media and prevent government censorship(MISA 2015:31). According to MISA Lesotho the state of media freedom seemed to have backtracked to nearly four decades ago, with increased polarisation of the broadcasting sector along the political lines. The Lesotho one year old, Broadcasting Dispute Resolution Panel was crippled by a weak legal framework and lack of financial independence, because its operations heavily depended on the Lesotho Communication Authority (LCA) budget.

5. Laws, Ethics and Code of Conduct relating to the media in Lesotho

Although Lesotho was the signatory of the international freedom of expression such as the Windhoek declaration and the UN Declaration of Human Rights, and her constitution enshrined freedom of expression, there was and still no specific set of laws that regulated the media. Instead, there were pieces of legislation which impacted on the media, as well as the principal proclamations introduced during archaic colonial rule (MISA 2012:47). As a result, the government ministers and other officials initiated libel and defamation suits against members of Harvest FM.

MISA/IFEX (2008:1) posited that this occurred at the end of suspension of the Harvest FM broadcasting license, instituted by the Lesotho Communication Authority from July 21st to October 21st 2008. The LCA suspended the license on the grounds that the Harvest FM station failed to comply with the broadcasting rules. According to MISA/IFEX (2008:1), the station was suspended for twelve months, but nine months were set aside on condition that the station did not commit the similar offence within that period.

Adding to the decline of freedom of expression in May 2008, the Lesotho Communications Authority increased the cost of broadcasting licenses sevenfold from $400 to $3000,drawing objection from press freedom advocates who claim that this was intended to deter more broadcasting players (Puddington, Piano, Neubauer and Roylance 2009:23).

However, MISA(2013:49) argued that although Lesotho civil society activists and media practitioners were happy about the vibrant expression of freedom of speech and viewed this as a credit in substance of democratic governance, there were some concerns about lack of professionalism, lack of ethics and poor moderation of programmes, particularly on some political talk shows. According to MISA Lesotho (2013:49) some radio stations were criticised for the unprofessional way they handled phone in programmes by allowing some callers to reveal secrets and lie about others. While one radio stations played recordings of the secret meetings of political parties and revealed some cabinet confidential documents through reading them word for word. While on the other hand the Directorate of Corporate and Economic Offences (DCEO), complained to MISA Lesotho, that some radio presenters handled the corruption issues in a manner that obstructed

the DCEO investigations.

MISA (2015: 31) pointed out that against the backdrop of political instability and uncertainty, Lesotho long waited media reforms continued to stall in 2014 and 2015. According to MISA the reform packages were the results of almost one and half decade's discussion between government and media professionals. MISA contended that these reforms could have depoliticised government owned media outlets and moved the statutes allowing government censorship in the name of national security and moved many slander and libel cases out of courts into arbitration.

6. The Role of Media in Democratic Society

Selinyane (2008:167) argued that media's influence in shaping the public's view of democracy was equally important as giving the citizens their freedom to choose to put forward their own line of thinking or reproduced and popularised political parties. According to Selinyane (2008:168), the privately owned media however exploited their freedom of expression by presenting inflamed information that might have steered instability in the country.

MISA (2015:32) posits that, most of the radio stations both government and private owned radio stations are controlled by politicians who use them as mouth pieces for advancing their political agendas. According to MISA the state owned television and radio stations were used by the three parties in government as their battlefield for the three political parties in the coalition government, while the privately owned were divided into congress and national ideologies. Despite prevalence of Windhoek declaration the radio presenters did not hide their political preferences and this was coupled with regularly expression of emotions and opinions about issues on, which they should have been maintaining neutrality and upholding professionalism and media ethics(MISA2015:32).

Access to communication is one of the key measures of power and equality in modern democracies. According to Bennett and Entman (2001:1) argued that people communicate to make their interests and values known and learn about the status of government activities affecting their interests. Due to its wide range of communication channels, contents and styles, media communication can shape power and participation in society in both

negative and positive ways. For instance, the dissemination of top-down communication can be used with negative effect in media to obscure the motives and interest behind political decisions; while on the other hand, it can be used positively for promoting involvement of citizens in decisions that affect their interests. Furthermore, participatory communication may either be integrated into government dialogues or categorically defined as a threat to national integrity, by different types of governments.

MISA2(2015:123) posited that with rapidly evolving information communication technology (ICTs) has expanded into the new and social media sphere and media outlets had the responsibility to extend the application of journalistic principles to these diverse platforms in order to take opportunity of the convergence. Whilst Lesotho Communications Authority (2008: 2) stated that the growth of the convergence between media outlets and information communication technology has brought both regulatory challenges and opportunities. The opportunity was that the consumers were able to make affordable calls while the challenge was the information code of conduct and ethics. Verdegem (2011:1) succinctly pointed out that the increasing independence on information and communication technologies (ICT) in every aspects of life, forced the world population to reflect on how they can manage the digital era with policies and try to explore conditions on how to benefit from new opportunities provided by ICT.

7. The Role of Radio in Promoting Audience Participation in Lesotho

Lesotho in the 1990s saw a shift from the state of print media domination role of information dissemination, due to the advent of radio that had a significant influence in shaping political information and public opinion. According to Lewis (1958:8), public opinion was conceived as part of social processes and contributes a way to chat the meaning of an emerging mass culture, and the power of mass media. Broadcast media in Lesotho was the most cost - efficient and accessed source of media for ordinary Basotho citizens (*UNDP, Human Development Report* 2009).

In a country such as Lesotho, with geographically remote areas, incomplete media coverage of most regions except the urban areas and an overall lower level of formal education with an89 percent literacy rate (Kingdom

of Lesotho. Bureau of Statistics, 2014:1), radio remains the most popular media platform due to the Basotho 'spoor culture of reading. Similane (1995:2) argues that the role of the media has been dominated by the strong beliefs about its potential as a means of influencing, controlling or directing public opinion.

Media content is determined by a number of editorial processes. Primarily, media content is characterized by editorial agenda setting. Agenda setting is the selection and display of the news by editors and news directors to influence public perceptions of most important issues of the day (Maxwell 2004:1). According to Maxwell, this reflected the authority of gatekeepers over content and therefore**,** the ability of gatekeepers to influence the topics on the public agenda. Similarly, MISA (2013:48) points out that radio stations in Lesotho have proven to be powerful in agenda setting and influencing people's perceptions.

Radio is the widest-reaching and most influential source of news and information globally. Furthermore, Fones-Wolf (2006:14) points out that radio stations were an instrument of the mass media that was indeed able to promote a new national self-awareness. According to Fones-Wolf, radio phoning was the most popular amusement in the United States; it epitomized consumer culture and grew the size of audience at a phenomenal rate, rendered radio an integral part of citizens' daily life(Fones-Wolf 2006:16). Hence, radio played a particular significant role in emerging public communication processes, because it facilitated information dissemination beyond the transport limits of print media (e.g. poor roads, printing times and equipment), sidestepping the literacy limits of near-illiterate audiences, as well as bridging, to some extent, the spiral of silence for audiences marginalised because of their education, remoteness or non-access to written forms of communication (African Media Barometer2011:54).

Additionally to the receiving of information, audiences contributed to programme content and feedback of radio programming through oral expression, thus they can overcome inherent limits to their education level. This was particularly significant in vernacular radio station programming where the mother tongue utilised, thus allowing audience members with low formal education to present their views and interacted with others as fully-fledged adult participants in the social context, without feeling inferior to those who may speak more languages and have better written skills,

especially in the regional language of English.

Coronel (2011:10) posits that in many new democracies, radio became the medium of choice as a less expensive and more accessible and effective instrument in promoting grassroots democracy, by providing an alternative source of information to official channels and reflecting linguistic diversity.

Conclusion

In this paper I concluded that in as much as Lesotho claimed to be a democratic country and enshrined freedom of expression in her constitution and also been a signatory of various conventions embraced the freedom of expression, She still had a serious challenge of information ethics and dilemma of code of conduct emanated from the absence of information law and media policy to guide the citizens in exercising their rights and their responsibilities when participated in cyber space and other media platforms like radio stations.

8. References

1. AfricanMediaBarometer.2010https://www.google.co.ls/?gws_rd=cr,sslandei=dyOoU7GzDo2w7Aa4soDQCw#q=african+media+barometer+lesothoandsafe=active[Accessed 15/06/2014] Bannet L W and Entman. R. M 2001. Mediated Politics eds Cambridge University Press New Yorkhttp://books.google.co.ls/books?id=L0GROJKLHukCandprintsec=frontcoveranddq=Bannet+%26Entmanandhl=enandsa=Xandei=l3WpU7SvGMeM7AbI2IDgDAandved=0CEEQ6AEwCA#v=onepageandq=Bannet%20%26Entmanandf=false[Accessed 12/06/2014]
2. Bureau of Statistics Lesotho. 2014. http://www.bos.gov.ls/ [Accessed 04/02/2015]
3. Christians, C. G,Glasser, and T. L, Mc Quail, D, Nordenstreng, K and White, R. A. 2009.Normative Theories of Media: Journalism in Democratic Societies. https://www.google.co.ls/search?tbm=bksandhl=enandq=normative+theories+of+mediaand=andgws_rd=ssl[Accessed 6/11/2014].
4. Coronel S .S. Role of the Media in Deepening Democracy http://unpan1.un.org/intradoc/groups/public/documents/un/unpan010194.

pdf[Accessed 23/06/2014]

5. Freedom House. 2011.Freedom of Press. https://www.freedomhouse.org/sites/default/files/FOTP%202011%20Final%20Full%20Report.pdf
6. *UNDP, Human Development Report* 2009. Lesotho Country Report. Accessed 12.08.2015. http://www.bti2010.bertelsmann-transformation-index.de/index.php?id=1406&tt_news=&type=98&L=0
7. MISA. 2013. So This Is Democracy?: State of Media Freedom in Southern Africa. http://www.misa.org/files/STID_2013_Lesotho.pdf[Accessed 30/04/2014].
8. MISA/IFEX .2011.Privately-Owned Radio Stations off the Air amid Demonstrations"
9. Lesotho. Minister of Communications, Science and Technology 2007. Opening Remarks of Hon. Minister of Communications, Science and Technology Mr. MothetjoaMetsing at a Workshopon the Role of Broadcasting in a Democratic Dispensation, Lesotho Sun, 24th August 2007. http://www.gov.ls/articles/2007/REMARKS_%20MINISTER_COMMUNICATIONS_Broadcasting.php[Accessed 06/02/2014]
10. Nordenstreng, K. 2007. Media and Society.Department of Journalism University and Mass Communication, University of Tampere.http://www.uta.fi/jour/english/contact/nordenstrengenglishhlm
11. Puddington, A ; Piano, A; Neubauer, K; Roylance, T. 2009. Freedom in the World 2009: The Annual Survey of Political Rights and Civil Liberties.http://www.amazon.it/s/ref=dp_byline_sr_book_1?ie=UTF8&field-author=Arch+Puddington&search-alias=stripbooks[Accessed 18/05/2015
12. Selinyane, P.N. 2008.Elections and Democracy in Lesotho: "The Media and Electoral Politics in Lesotho between 1993 and 2007".Vol.7 (1) EISA.

Intellectual Freedom and Censorship in the Eyes of Nigerian Law

by Mercy Ifeyinwa Anyaegbu[1] & Nneka Obiamaka Umejiaku[2]

1. Overview of intellectual freedom and censorship

Intellectual freedom according to Article 19 of United Nations Universal Declaration of Human Rights is the right to freedom of thought and of expression of thought. Clearly it is stated in this Declaration that:

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

Similarly, the American Library Association describes intellectual freedom as the right of every individual to both seek and receive information from all points of view without restriction. It thus provides for free access to all expressions of ideas through which any and all sides of a question, cause or movement may be explored.

The concept of intellectual freedom involves protecting the rights of all individuals to pursue the types of information they want and to read anything that interests them (Yaya, Achonna & Osisonwo, 2013). Intellectual freedom not only guarantees individuals the right to hold opinion on any subject but also the right to communicate such ideas in any media of one's choice without any restriction. Intellectual freedom can only exist where two essential conditions are met: first that all individuals have the right to hold any belief on any subject and to convey their ideas in any form they deem appropriate and second, that society makes an equal commitment to

1 Deputy Law Librarian, Faculty of Law Library, Nnamdi Azikiwe University, Awka, Nigeria, E-mail: ifymanyaegbu@yahoo.com.

2 Lecturer, Department of Commercial and Property Law, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria, E-mail: nnekaumejiaku@gmail.com.

the right of unrestricted access to information and ideas regardless of the communication medium used, the content of the work and the viewpoints of both author and the receiver of information.

It could be seen normally that intellectual freedom, therefore, deals with the right to speak and think without restriction. In the struggle to ensure that individuals' right to both access and use information in public institutions is guaranteed, IFLA (The International Federation of Library Associations and Institutions) states:

- That human beings have a fundamental right of access to expressions of knowledge, creative thought and intellectual activity, and to express their views publicly.
- That the right to know and freedom of expression are two aspects of the same principle. The right to know is a requirement for freedom of thought and conscience; freedom of thought and freedom of expression are necessary conditions for freedom of access to information.
- That a commitment to intellectual freedom is a core responsibility for the library and information profession.
- IFLA therefore calls upon libraries and library staff to adhere to the principles of intellectual freedom, uninhibited access to information and freedom of expression and to recognize the privacy of library user. IFLA urges its members to actively promote the acceptance and realization of these principles. In cases of conflict between these responsibilities, the duty towards the user shall take precedence.

The Kampala Declaration on Intellectual Freedom and Social Responsibility is involved in the struggle to promote intellectual freedom among the academic community. In Article 9, it states that the intellectual community shall have the right to express its opinions freely in the media and to establish its own media and means of communication. Again in Article 10,

> *all members of the intellectual community shall have the freedom of association, including the right to form and join trade unions. The right of association includes the right of peaceful assembly and formation of groups, clubs and national and international associations.*

The protection of intellectual freedom was also strengthened by Article 15 which states *inter alia* that the State shall desist from exercising censorship

over the works of the intellectual community.

2. Benefits of intellectual freedom in Nigeria

The importance of intellectual freedom in the growth of any society is fundamental. Intellectual freedom is the bedrock for other freedoms- speech, expression, and the press. In a democratic system of government as practiced in Nigeria, the citizenry should form part of the government; for it is believed that power to change any government lies with the electorate. The citizenry should be well informed not only to elect their leaders but to also make meaningful input in governance, join in public debates and criticize the policies of the government where necessary. Access to the right information at the right time will produce the necessary result. Thus intellectual freedom encompasses the freedom to hold, receive and disseminate ideas without restriction.

Intellectual freedom is not only necessary to adult members of the society but also to younger ones, especially adolescents. These teenage groups have varying information needs. Adolescence according to Calkin (2014) is a time of vast neurological, physiological, emotional and social change. Teenage brains are primed for learning and more open to new experiences. Calkin informed that adolescence is an age group more interested in novelty and new sensations than human brains at any other developmental stage of man. They are restive in nature. They have insatiable quest to understand and grapple with the changes in their body mechanism as well as the perplexities they found in their environment. They like to explore and carry out experiment on their own in order to form an independent view of life. They need access to information on a wide range of topics that will depict a wide range of experiences. Such unrestricted access to information can only be guaranteed by intellectual freedom.

Major constraints why Nigerian citizens seem not to bother much about intellectual freedom are simple to enumerate. They include:

- Illiteracy
- Ignorance
- Poverty
- Fear of victimization
- Poor ICT skill and infrastructure and

- Lack of political will

3. Censorship

Censorship is the direct opposite of intellectual freedom. According to Harshrustic (2007), censorship is the act or practice of suppressing the speech or public communication which is considered objectionable, harmful and sensitive, by a government, media outlet or other controlling bodies. Reichman (1988) defines censorship as the removal, suppression or restricted circulation of literary, artistic or educational materials on the grounds that they are morally or otherwise objectionable in the light of standards applied by the censor. He explained that virtually any decision made by school board members concerning what is taught, used and learned in school can be viewed as censorship. By this he means that when a superior authority prescribes what is to be taught or read censorship occurs. Dafiaghor (2011) summed it thus:

Censorship is based on the fact that every society has customs, taboos or laws by which speech, dress, religious observance and sexual expressions are regulated in order to protect the family, the church and the State. In the light of this, Reichman (1988) gave a more elaborate definition of censorship as the examination of books, plays, films, television and other forms of communication for the purpose of altering or suppressing ideas found to be objectionable, harmful or offensive. Information materials could be censored either prior to publication or after publication. Censorship can also be carried out either by negotiation or through force by the government or its agencies, individuals, organizations, religious groups or other associations. In Nigeria, reasons for censoring an information material may exist to protect the State or for the protection of the family. Dafiaghor (2011) identified the following types of censorship usually carried out in Nigeria as:

- Moral Censorship
- Military Censorship
- Political Censorship
- Religious Censorship
- Corporate Censorship

These are the major social institutions in Nigeria that censorship is meant

to protect. The effect on any of them would definitely affect the other because they operate as interdependent units of the Nigerian nation.

3.1 Censorship can be beneficial

Censorship appears to have some negative effect on access to information materials, but it also has some beneficial effect more especially to adolescents. Some writers believe that censorship has some beneficial effect. Hastings (1990) believes that censorship which promotes good, virtuous character and condemns pervasive thoughts, words and conduct is good and desperately needed in our nation. He believes that freedoms which are abused and misused should be taken away. Those acts which impact negatively on people's behaviour should be censored. According to him, those who advertise their products know that it is important to get their message into the minds of others. For instance, pornography encourages violent sexual acts such as rape, child molestation, incest e.tc.

Other people believe that censorship exists to protect vulnerable groups like adolescents and children. They believe that growing youths should not gain access to sites with sexual content or inappropriate violent websites that might lead the teenagers the wrong way. Without censorship children and teens would be able to see disgusting things on the television and on the Internet. Such things as porn videos would be turned into TV shows where people could see it. There would be too much violence on TV (2016 Debate.org). Equally without censorship, people would be able to see body parts and things like that on the television. Hence censorship exists to protect large masses of people from damaging content in public media. Some of the advocates of censorship strongly believe public content is censored to control obscenities, protect young people from pornography, promote or restrict political or religious views and national security.

4. The protection of intellectual freedom in the 1999 Constitution of the Federal Republic of Nigeria

Chapter 4 of the *1999 Constitution of the Federal Republic of Nigeria* dealt extensively on fundamental rights of the citizenry. Specifically in Section 34(1), it states that:

> *Every individual is entitled to respect for the dignity of his person. No person shall be subjected to torture or to in human or degrading treatment. Again no person shall be held in slavery or servitude or required to perform forced labour or compulsory labour except on conviction by order of court.*

In Section 35 where the Constitution provides that every person shall be entitled to his personal liberty and that no person shall be deprived of such liberty save in the execution of a sentence of a court in respect of criminal offence of which he has been found guilty or for health grounds (for infectious or contagious diseases) or for the purposes of education or welfare of minors and to prevent unlawful entry into Nigeria.

Furthermore, section 37 guarantees and protects privacy of citizens, their homes, correspondence, telephone, conversations and telegraphic communications. Mainly this section deals with the right to private and family life.

Under section 38(1) of the *1999 Constitution of the Federal Republic of Nigeria* that every person shall be entitled to freedom of thoughts, conscience and religion, including freedom to change his religion or belief and freedom either alone or in community with others, and in public or in private to manifest and propagate his religion or belief in worship, teaching, practice and observance.

The Constitutional provision in Section 38(2) forbids censorship on religious grounds. No person attending any place of education shall be required to receive religious instruction or to take part in or attend any religious ceremony or observance if such instruction, ceremony or observance relates to a religion other than his own or a religion not approved by his parent or guardian.

In practice this right has been abused and violated by some religious sects in Nigeria. A case in hand is the abduction of the Chibok girls by members of Boko Haram in 2014. Under section 38, censorship of religious beliefs and instruction is prohibited in Nigeria. Section 38(4) is however a form of censorship for persons who desire to be a member of a secret society; although the definition of secret society is somehow silent in the Constitution.

Right to freedom of expression and the press is protected in section 39. In subsection (1) the Constitution states that every person shall be entitled

to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference. Consequently in section 39(2) the constitutional provision is that every person shall be entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions.

Intellectual freedom is the bedrock for other freedoms such as freedom of expression, freedom of speech and freedom of the press. A cursory look at the constitutional provision in section 39 would seem that the Nigerian law promotes intellectual freedom. Depending however on the government in power, this right is not always exercised in full by citizens of the country. Successive governments have clamped down on this right- freedom of expression. *Per se* there is no provision in the 1999 Constitution that prohibits freedom of expression but in everyday life, the government has been doing that in a subtle way. Individuals who have publicly expressed their displeasure at government policies have had their rights infringed as a result. The provisions of the *Economic and Financial Crime Commission (EFCC) Act* and other related laws have been invoked on political opponents who publicly criticized the government of the day. Presently a good number of members of the opposition party; The Peoples' Democratic Party have been incarcerated in the past few months for criticizing the government publicly. The leader of Movement for the Creation of the Republic of Biafra has been remanded in prison custody despite the bail which the Court has granted him. Court orders (for the freedom) are not respected by the government in cases of such persons who publicly expressed their displeasure at government policies. Thus human rights of political opponents who criticize the government publicly is infringed.

5. National Film and Video Censor Board Act, 1993 and National Film and Video Censors Board Regulations, 2008

This Act was established to empower the *National Film and Video and Censors Board* to regulate the censorship and public exhibition of films and video works and matters connected therewith. The Board was empowered to censor films and video works. Secondly, it could launch new censorship and classification guidelines to aid film makers and professionalize the operations of the Board. It is stated in section 5(1) of NFVCB Regulations, 2008 that no one shall exhibit, distribute, cause or allow to be exhibited or

distributed a musical video unless a censorship certificate has been issued by the Board. In addition, section 5(2) states that each musical video track in a musical video recording shall be considered a short length film to be censored and classified independently. Thus the film and video industry though mainly in the domain of private persons is censored in Nigeria.

6. The Criminal Code on obscene publications

The Criminal Code prohibits the use of obscene publications in public media in Nigeria. In Section 233C (1) of the Act, an article shall be deemed to be obscene or the purposes of this Chapter if its effects taken as a whole is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. Subject to the provision of Section 233 D (1) any person who, whether for gain or not, distributes or projects any article deemed to be obscene for the purposes of this Chapter, commits an offence punishable on conviction by a fine not exceeding four hundred naira or by imprisonment for a term not exceeding three years or by both.

A plethora of other Nigerian laws such as the *Official Secrets Acts, The Criminal Code Act*, the *Penal Code, Evidence Act, the Public Complaints Commission Act,* all made provision for penalties for unauthorized disclosure of information in public institutions. Interestingly, salient sections of the *Freedom of Information Act* (which was enacted after prolonged session of debates and struggle which ended in May, 2011) overrides the sanctions in these Acts.

7. Freedom of Information Act 2011

The Freedom of Information Act was enacted by the National Assembly and assented to by President Goodluck Ebele Jonathan in May 2011. It was an Act to make public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse consequences for disclosing certain kinds of official information without authorization and establish procedures for the achievement of those purposes and for related matters.

Section 1(1) made provision for the right of any person to access or request information in whatever media which is in the custody or possession of any public official, agency or institution. Under section 1(3) of the Act, an applicant has the right to institute a legal action in the Court to compel any public institution to comply with the provisions of the Act. Under this Act, request for access to such information shall be granted within 7 days as contained in section 4. Where access to such information is denied, reasons for such denial shall be stated in writing as provided in section 7. Grant of access to information requested is free except to cover the processing expenses.

Acceptable reason for the denial of access to information in the Act as contained in sections 11, 12, 14, 15, 16, 17, 18, 19, 20, 21 is for information that refer to international affairs, defense, law enforcement and investigation, personal information, third party information, trade secrets, research materials etc. Information materials exempted from this Act are contained in section 26. They are published materials, library and museum materials meant for exhibition. Public officers who grant access to requested information in their possession are protected from the *Official Secrets Act, Criminal Code, Penal Code* etc in section 27 of the Act. Notwithstanding the provisions of sections 11-19, access to requested information must be granted if it is for the overriding public interest.

To promote intellectual freedom, this Act made provision in section 4 that a public institution shall ensure that information in its custody or possession is widely disseminated and made readily available to members of the public through various means, including print, electronic and online sources and at the offices of such public institutions. Such public institutions are also required to update and review all such information and effect changes whenever they occur. Furthermore, section 13 made provision for every government or public institution to train its officials on the public's right to access information or records in its possession as well as for the effective implementation of this Act.

8. Draft bill to prohibit frivolous petitions and other relevant matters

Recently, the Deputy Senate Leader, Senator Bala Ibn Na'allah sponsored a bill aimed at setting out heavy sanctions for persons who falsely criticize

public officials or institutions. This bill seeks to forbid social media operators from slandering members of the public including lawmakers.
Highlights from the bill include:

> *Notwithstanding anything contained in any law, it shall be unlawful to submit any petition, statement intended to report the conduct of any person for the purpose of an investigation, inquiry or inquest without a duly sworn affidavit in the High Court of a State or the Federal High Court confirming the content to be true and correct and in accordance with the Oaths Act.*

Similarly, any petition and or complaint not accompanied by a sworn affidavit shall be inadmissible and shall not be used by any government institution, agency or bodies established by any law for the time being enforced in Nigeria. The bill further stated that:

> *Any person who unlawfully uses, publishes or causes to be published, any petition, complaint, not supported by a duly sworn affidavit, shall be deemed to have committed an offence and upon conviction, shall be liable to an imprisonment for six months without an option of fine.*

Further sanction for offenders include: any person who acts, uses or causes to be used any petition or complaints not accompanied by duly sworn affidavit shall be deemed to have committed an offence and upon conviction, shall be liable to an imprisonment for a term of two years or a fine of ₦200,000 (two hundred thousand naira) or both. It also states that where any person in order to circumvent this law makes any allegation and or publish any statement, petition in paper, radio or any medium of whatever description, with malicious intent to discredit or set the public against any person or group of persons, institutions of government, he shall be guilty of an offence and upon conviction, shall be liable to an imprisonment for two years or a fine of ₦4, 000,000.00 (four million naira).
For the social media, the bill states that:

> *Where any person through text message, tweets, WhatsApp or through any social media, posts any abusive statement knowing same to be false with intent to set the public against any person and group of persons, an institution of government or such other bodies established shall be guilty of an offence and upon conviction shall be liable to an*

imprisonment for two years or a fine of ₦2,000,000.00 (two million naira) or both fine and imprisonment.

This bill has gone through second reading at the floor of the Senate. Since the inception of the bill, there has been a public outcry from members of the press, civil society groups and the Nigerian public. All the criticism is based on the assertion that the bill is a ploy by the government to undermine freedom of expression, freedom of speech, freedom of the press and public participation in governance and democracy. In the words of Ndukwu (2015), the bill constitutes a threat to democracy because it seeks to repress the social media, the conventional media, the civil society and the citizenry as a whole. If passed into law, it will violate the norms of democratic practice, freedom of expression, press freedom, transparency and accountability as well as open governance.

In Nigeria, this is the most recent move to entrench censorship. If it succeeds it will stifle intellectual freedom in the country. Some civil society groups in Nigeria have petitioned the United Nations against the bill.

9. Recommendations

Based on issues raised in this discourse, the following recommendations were made:

1. Nigeria is a signatory to many international Conventions that advocate the entrenchment of fundamental human rights. As such, Nigeria should review and repeal relevant sections of Nigerian laws that negate intellectual freedom. The fines prescribed in some of these laws like in the *Criminal Code* should be reviewed upward in view of the current economic realities in Nigeria.
2. Most censorship practices in Nigeria are anchored on religious belief, morality and ethics. In view of our cultural practices and heritage, laws that prohibit abortion, same-sex marriage, public display of pornography and obscene materials should be upheld.
3. Current debate on the prohibition of frivolous petition and other matters before the Nigerian senate should be suspended. A concerted effort should be made by the Executive arm of the Government, the civil society groups, members of the press and the entire Nigerian citizens to

ensure that that bill is not passed into law. It is an affront to intellectual freedom.

4. Many Nigerians are not aware of what intellectual freedom is as well as the benefit of this freedom. Public enlightenment both by the government and civil society groups is necessary, if not mandatory, in this struggle.
5. Intellectual freedom is better appreciated by an educated populace. Free and compulsory education up to senior secondary school level should be made a law in Nigeria. Presently both the educational and political objectives of the Federal Republic of Nigeria as enshrined in chapter two of the 1999 constitution are not justifiable, as the government cannot be sued for non compliance.
6. The level of ICT skills and infrastructure in the country is still poor. As such some of the information that transpires via the electronic media is missed out by many Nigerian citizens. Many are not aware of some of the debates that tend to infringe on their fundamental human rights by the state and national assemblies until they become law.
7. The Nigerian libraries, more especially public libraries should be better resourced through improved funding. The public library by its nature is a library for all and a lay man's university. Live debates happening at the state and national assemblies can be viewed by users at the library.
8. The enactment of the Freedom of Information Act in Nigeria is expected to promote intellectual freedom in principle. A major drawback of that law is in the enforcement. The country should set up a regulatory body to monitor the implementation of the provisions of that Act.

9. Conclusion

Intellectual freedom is a principle sustaining the right to say, do, and think without restriction while censorship is the direct opposite. Most laws that encourage censorship in Nigeria are anchored on religious beliefs, morality and ethics. When freedom of expression in one country is affected, it may inhibit access to information in other countries. Thus, the defense of intellectual freedom requires a universal effort from various nations of the world through the instrumentality of their local legislation.

10. References

1. Calkins, E. (2014) The right to read: The how and why of supporting intellectual freedom for teens. Retrieved from http://www.inthelibrary-withtheleadpipe.org/2014/the-right-to-read-the-how-and-why-of-supporting-intellectual-freedom-for-teens/.
2. Dafiaghor, K. F. (2011) Censorship of information and the Nigerian society. *International NGO Journal* 6 (7), pp. 159-165.
3. Draft Bill to Prohibit Frivolous Petition and Other Matters Connected Therewith.
4. Fobour, Y. A. (2014) Balancing the Same Sex Marriage (Prohibition) Act, 2014 with fundamental human rights in Nigeria. *National Human Rights Commission Journal* 4(12), p. 78.
5. Freedom of Information Act, 2011.
6. Harischrustic, (2007) Censorship does both harm, good. Retrieved from https://www.waterlook12.ia.us/schoolsites/the spectator/censorship-does-both-harm-good.
7. Hastings, D. R. (1990) Censorship can be beneficial. Retrieved from http://www.truthmagazine.com/archives/volume34/GOTO34300.html p.1
8. IFLA Statement on Libraries and Intellectual Freedom, 1999.
9. Kampala Declaration on Intellectual Freedom and Social Responsibility, 1990.
10. National Film and Video Censors Board Act, 1993 (Cap N40) LFN 2004.
11. National Film and Video Censors Board Regulations, 2008.
12. Ndukwu, E. (2015) Senate and the opposition against anti-social media bill. *National Mirrow.* Retrieved from http://nationalmirrowline.net/new/senate-and-the-opposition-against, p. 2.
13. 1999 Constitution of the Federal Republic of Nigeria (as amended).
14. Reichman, H (1988) Censorship and selection, issues and answers for schools. Arlington: AALS, p. 141.

The Nigerian Information Act 2011: A Veritable Tool for Good Governance

by Ifemeje Sylvia Chika[184] *& Odoh BenUruchi*[185]

1. Introduction

In 2011, the Nigerian government signed the revolutionary Freedom of Information bill into Act. By virtue of this, Nigeria became the ninth country in Africa and among over 90 countries in the globe to enact this Law (Dunu, et al. 2014). Freedom of information, especially as it pertains to access to information held by public authorities, is a fundamental element of the right to freedom of expression and very vital to the proper functioning of a democracy as it curbs executive, judicial and legislative recklessness. This Act under discourse makes provision for disclosure of information held by public authorities or by person providing service for them (Robert, 2000). The passage of this all important Act was heralded by all and sundry in Nigeria, because it not only reduced the risk of obtaining and releasing information held by government and public institution, the Act equally affords the citizen the opportunity to participate in governance and with this legislation in force the era of official secrecy backed by law has been effectively and decisively dethroned and transparency and accountability enthroned. Stephen Harper, Canadian opposition leader has rightly observed in 2005:

> *Information is the life blood of a democracy. Without access to key information about government policies and programs citizens and parliamentarians cannot make an informed decision and incompetent or corrupt government can be hidden under a cloak of secrecy.*

184 Associate Professor ofLaws, Department of International Law and Jurisprudence Faculty of Law NnamdiAzikiwe, University Awka Nigeria.

185 Lecturer, Department of Public Law Faculty of Law, Nigerian Police Academy Wodi Kano Nigeria.

The above observation made by Harper is apparently more pertinent to under- developed countries like Nigeria, where corruption and official secrecy is the order of the day. The Act therefore no doubt is an indispensable tool in the hands of the media; human right activists and the civil society to fight corruption and ensure that public institution in Nigeria adopt a governance process that is not only accountable and transparent but also responsive to Nigerians. This paper therefore, as the title depicts, aims at discussing the rationale for the enactment and implementation of the Act. The paper also dissects some of the legal decisions or pronouncement on this landmark Act. Finally, the paper highlights some drawbacks, challenge or clogs in the wheels of the Act, which has succeeded in creating a wide yearning implementation gaps. Recommendations shall be proffered on how best Nigerians can harvest the full benefits of this historic legislation.

2. The emergence of Nigerian Freedom of Information Act

The modern concept of Freedom of Information Act (FOI) is traceable to the United Nation Universal Declaration of Human Right (UNDHR) (Udofa, 2011). Article 19 0f the 1948 Declaration provides:

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through media regardless of frontiers.*

Before 2011, Nigeria enshrined the right to freedom of speech in section 39 of her Constitution. However, there was a spectrum of Law in place in Nigeria which hindered the media and public from having access to records of the government and vital information that were classified as official and thereby privileged. These Laws in question criminalized the act of civil servants divulging official facts and figures to the Public or Journalist. Apparently, they were relics we inherited from our colonial masters. Ironically, the laws in question have since been over -hauled in Britain but for a long time Nigeria kept on clinging unto these obsolete laws. For example, the Nigerian Official Secret Act which has been amended expressly by Section 27 FOI Act, made it an offence for a civil servant to give out government information. Sections 190 and 191 of Evidence Act made certain

communications on state affairs to be privileged. Section 190 provides, for instance, that before the production of records pertaining to the affairs of the state, the directions of the President or that of the State governor as the case may be must be sought. Section 191 equally provides that a public officer cannot be compelled to disclose communication made to him in official confidence, if he consider that doing so will jeopardize the public interest. However, the Evidence Act happily provides a proviso to the effect that the head of the Ministry, Department or Agency may be ordered by the court to provide the document to the judge alone in chambers. Furthermore, both the Nigerian Criminal and Penal Codes, also made it a crime for a person to divulge public information without proper authority.

It was against this backdrop of the prevalence of draconian laws that hindered the rights of the public to access government information that the FOI Act 2011 came into existence. The idea of Freedom of Information Act, was conceived sometime in 1993 by three different organizations independently: the Media Right Agenda (MRA), the Civil Liberties Organisation (CLO) and the Nigerian Union of Journalist (NUJ), they agreed to work together on a campaign for the enactment of a Freedom of Information Act. The main objective of the campaign was to lay down as a legal principle the right to access documents and information in the custody of the government or its officials and agents as a necessary corollary to the guarantee of freedom of expression. It also was aimed at creating mechanisms for the effective exercise of this right (Ali Yusuf, 2014). Following extensive research, Media Right Agenda Legal Directorate headed by Mr. Tunde Fagbohunmi of the Law firm of Aluko and Oyebode produced a draft bill in 1994 titled "Draft Access to Public Records and Official Information Act". This eventually translated into Freedom of Information Act after many modifications.

After five years of legislative process, the Freedom of Information Act was passed into law on the 28th May 2011. The Act established a "Right to know" legal process, which allows request to be made for government-held information, which could be received after the payment of standard charges for document duplications and transcription where necessary. On the passage of the bill, it created a record of being the oldest and most controversial Bill that had ever come before the Nigerian National Assembly. The bill would have been passed in November 2006, but the then Nigerian President, Obasanjo refused to give his assent, on the ground that it con-

stituted a security threat and he also disagreed with the title of the Bill. It was not until 2011 that President Goodluck Jonathan gave his assent. Before 2011 Nigeria regarded FOI Act as a luxury only practicable in Western world and other established democracies.

3. Salient Innovations of Nigerian FOI Act 2011

With the emergence of the FOI Act 2011, the era of official secrecy backed up by Law was effectively jettisoned. The FOI Act interalia succeeded in amending sections of the Secrecy Act 1911, which impedes the right of any person to access information which is in the custody or possession of any public official, agency or public institution. By virtue of section 1(2) of the FOI Act, an applicant need not demonstrate any specific interest in the information being applied for. Again, the Act ensures access to public information to all irrespective of age, race, status or gender. Also the reason for wanting that information was made irrelevant. Another important feature of the FOI Act is the criminalization by the Act of destruction of records under section 10. The Act in section 2(4) equally mandates public institutions to proactively disclose information within its custody. The Act also protects "whistle blowers" in public service who release in good faith any information pursuant to FOI Act, especially where there is failure of public duty, abuse of power or mismanagement of public resources or corruption. Section 13 of the Act provides for the government or public institution to offer appropriate training for its officials on the public's right to access information or records held by government for the effective implementation of the Act. The Act creates reporting obligations in compliance with the Law for all institutions affected by it. Reports are to be made annually to the Federal Attorney–General Office, which will in turn make them available to both the National Assembly and the Public. The Act, furthermore, in section 29(5) requires the Federal Attorney- General to oversee the effective implementation of this duty to the Parliament annually (Afolayan, 2012).

Another salient innovation of the FOI Act is the recognition of a range of legitimate exemptions and limitation to the public right to know. Under Sections 11(1), 12(1) and 16 FOI Act, someinformation may be withheld in order to protect certain interests which are allowed by the Act. If this is

the case, the public authority must explain why the information is withheld or provide the information within seven working days. Section 28, equally prohibits the initiation of civil or criminal proceedings against any person receiving the information or further disclosing it.

Finally non- denial of right to access information is now actionable, any applicant under Section 20 of the FOI Act who has been denied access to information or a part thereafter may apply to the court for a review of the matter within thirty days after the public institution denies or is deemed to have denied the application.

4. An overview and legal analysis of judicial decisions on FOI Act after four years of implementation

How did our courts enforce the strict implementation of this Act after four years of its enactment in 2011? The Federal High Court in Lagos had the first opportunity to interpret and apply FOI Act in the case of Boniface Okezie v. Central Bank of Nigeria[186]. In 2012, the Progressive Shareholders Association of Nigeria represented by Boniface Okezie wrote to the Central Bank requesting information relating to the recovery of Oceanic Bank Plc assets. The CBN refused to disclose the information requested by the Association. A suit was instituted under FOI Act by the association requesting the court to compel the bank to publish its handling of approximately N191 billion worth of assets forfeited by Ibru. In a landmark ruling the court held that the CBN, as a public institution has a duty under the Act to provide details of such information and that the bank'srefusaltodisclosetheinformationonrequestbytheassociationwasunlawful.

Justice Mohammed Idris therefore, ordered the bank to comply with the association's requestbyreleasing the information sought. The judge observed: "The Act is intended to promote transparency and prevent corruption. Therefore all public institution must ensure that they comply with the FOI Act in the interest of transparency, justice and development". The court, however, declined to compel the bank to disclose the information relating to fees and commissions paid to the Law firms representing the bank as such client/legal Practitioner's information is privileged under the

186 iLAW/CA/L/693/2010, www.ilaw.com.ng

Evidence Act.

In 2014, in an unreported suit, filed by Legal Defence and Assistance Project, some States of the Federation (Lagos, Imo, Rivers, Akwa Ibom and Delta). The application to the court arose as a result of the States refusal to disclose information to the plaintiffs bordering on the amount raised and received by the respective States from the Nigerian capital market through public offers or private placements between 2007 and 2011. The applicant's prayer essentially was for the court to compel these States (defendant) to provide the requested information pursuant to section 2 of the FOI Act 2011.

The Federal High Court in Lagos presided by Justice OkonAbang in a very disturbing judgment stated that the FOI Act 2011 was not binding on the 36 states of the Federation. Given the importance of the Act, it is quite upsetting that the court should pass such a retrogressive verdict. The importance of this Act can never be over-emphasized; it guarantees the freedom of Nigerians to obtain information from the government and its agencies. It also checkmates the cankerworm called corruption in governance. Therefore, any clog at all in enforcing the Act nationwide would be definitely counter-productive and would negate the whole essence of the Act. Happily, the Enugu State Federal High court in a case filed by libertiesorganization (CLO) against Enugu state Health Commission held that states are bound to obey the FOIAct.

Despite this positive legal development, this area of the Law is still in a state of confusion, and unsettled as the two conflicting decisions were delivered by courts of coordinate jurisdiction. It is time the Nigerian Court of Appeal came up with an overriding decision in order to put to rest this issue of non-applicability of the FOI Act to all the federating States of Nigeria.

5. Challenges hindering the full implementation of FOI Act 2011

While it is conceded that the journey so far is quite encouraging, there are still many hurdles that need to be surmounted; many yearning enforcement gaps that need to be filled. In a nutshell there are still numerous challenges hindering the full harvest of the benefits of this innovative Act. The challenges or draw backs are therefore discussed.

5.1 Non-domestication of FOI Act by the federating States of Nigeria

Unless the Federal Court of Appeal comes up with a definite decision on the enforceability of FOI in all the 36 states of Nigeria, the rationale behind the enactment of the Act would have been defeated. According to (Shosanya, 2015), stakeholders are worried about the conflicting judicial ruling dished out by our Federal High Courts. These divergent interpretations according to him would not only have a dysfunctional effect on the Act, but would also succeed in shutting citizens out of what is happening in government circles. As at 2014, only three states in Nigeria, Lagos, Ekiti and Delta, had adopted FOI Act. This is certainly not encouraging.

5.2 Exemption of certain information from public disclosure

The content of the Bill was watered down before President Goodluck Jonathan agreed to give his assent. For instance, it has been argued that section 28 of the Act, now gives Public Officers the discretion to classify certain information as not being covered by the Act and therefore not to be disclosed. Furthermore, it is equally argued that sections 11 to 17 of the FOI Act contain exemptions which ought to be covered by the Act (Ladan, 2012). It would be recalled that the rationale for establishing the FOI was to unveil the secrecy with which the public servants conceal the ordinary operations of the government and public institution. Such exemptions defeat the spirit behind the enactment of the Act.

5.3 Increased violent attack of journalists

While applauding the passage of the FOI Act, it has been observed that the publication of such hitherto hidden information has led to increased incidences of extra judicial killing, harassment and other forms of human rights violations against members of the public, especially journalists who have been previously given access to government information. For example, since 2011, This Day newspaper and a Media organization in Nigeria have suffered bomb attacks at Abuja and Kaduna respectively, suffering human and material losses. There is therefore an urgent need for the Nigerian government to beef up the state of security in the country, in order to create a violence freeenvironment that will facilitate or encourage reportage of in-

formation received without fear of any form of molestation or harassment.

5.4 Unwillingness of public officials to divulge government information

Outright, unsubstantiated refusal or inordinate delay by government officials to disclose information has been observed in some government institutions. Most officials will always reply "no comment" or switch off their phones thereby circumventing the full implementation of the Act. Besides, government workers that have tried to be compliant with the provision of the Act, have faced severe sanction from their superiors. Furthermore, outright denial of access to government information has invariably led to expensive and protracted litigation.

5.5 Lack of awareness of the import of the Act by a majority of the public

Many Nigerians are unaware of the existence of FOI Act as a result of lack of awareness-raising programmes to enlighten the Public on the import of the Act. The Act should be widely published and circulated, in order to facilitate easy access by the public through street book vendors.

5.6 Non-compliance with proactive disclosure of information by public institutions

Besides the statutory requirement of expeditious response of Public institutions to the demand to access information in their custody, section 2 (3) of the Act also compels public institutions to proactively publish extensive information about their operations and structure. However, most public institutions in Nigeria have not fully complied with this provision. The need for proactive disclosure is very crucial under this new dispensation. Where public institutions comply with this requirement of proactive disclosure, they are more likely to experience drastic reduction in the volumeofrequests for information that ordinarily would have come to them for disclosure. Udofa opines that such proactive disclosures will boost the confidence and trust of citizens in the government and governance.

5.7 Poor record-keeping by public institutions

Despite the present computer age, most public institutions have failed to computerize their records. Their records are still only paper-based. This invariably makes it practically impossible for them to comply with the mandatory seven days statutory period of releasing information to an applicant. Most of these institutions also lack proper cataloguing andarchiving.

5.8 Low compliance with yearly mandatory reporting obligations by public institutions

Section 29(3) of the FOI Act, enacts for yearly reporting to the Attorney-General by the Public institutions of compliance with the provisions of FOI Act. This is expected to serve as a way of checkmating compliance with the provisions of the Act. A request, however, made by Right to know (R2K) between April and June 2012, 18 months after the Implementation of the Act revealed that only 23 Ministries submitted annual compliance report to the Attorney-General and only 11 out of the 23 ministries have designated staff to handle FOI requests. This lackadaisical attitude of our government officials has been roundly criticized by (Udofa, 2012) as not acceptable. Udofa further stressed that public institutions ought to view more seriously their obligations under the FOI Act in order to ensure implementation of the Act, which is open democracy andgovernance.

5.9 Protracted and expensive cost of litigation

Non-disclosure of public information on requests invariably leads to protracted and expensive litigation thereby defeating the Act. Udofa (2012) has opined:

> *That the dragging of requests for information through the long application process from the High court all the way to Supreme Court has a potentially negative effect on the utility of the informationrequested.*

Therefore proactive disclosure or voluntary disclose is the better option that will facilitate the growth and smooth implementation of this Act.

6. Recommendations

Access to information is fundamental to the health and development of democracy. It not only ensures that the citizens make responsible, informed choices. It equally ensures that the elected representative or government officials carry out the wishes of the citizens. For journalist, it is a veritable indispensable tool, as the era of speculative reportage is gone. The FOI Act has given journalist access to the information they want, subject to few exemptions. As observed earlier however, in the course of implementation of this Act, after four years of it enactment, it has been observed that many constraints or obstacles have been encountered. It is highly imperative that these challenges are dealt with decisively in order to achieve the lofty ideals of the FOI Act. To this extent the paper suggests the following recommendations that will ensure that Nigerians reap the full benefits of theAct:

1. Public institutions should proactively disclose all classes of information mandated by FOIAct.
2. Public institutions should create and update their web sites at very frequent intervals in order to reduce incessant and endless requests from thepublic.
3. Public institutions should ensure non-destruction of government record irrespective of the age of thedocument.
4. Public institutions should comply in time with all the requirement of the FOI Act on the submission of reports and compliance with annual compliancereport.
5. The Attorney–General should ensure public institutions comply with the provisions of the Act in order to avoid unnecessary litigation.
6. There should be awareness raising programmes on the existence and import of the Act. The public should beenlightened.
7. The Court of Appeal should come up with specific pronouncements on the applicability of the FOI Act to every state inNigeria.
8. The Nigerian government should inhibit security in the country in order to the tide of violence that often intensify the reportage of sensitive governmentinformation.
9. Public institutions should timeously disclose information requested by the public. It is quite amazing and ironical that the National As-

sembly which passed the FOI Act has legally challenged the Federal High Court decision compelling it to respond to the requests for information about their salaries and emoluments. Public institution are advised to proactively and routinely comply with the provisions of FOI Act on proactive disclosure disclose in order to reduce the volume of requests that they willentertain.

10. All the records of Public Institutions should be computerized and updated at regular intervals. There should also be proper archiving and cataloguing in order to facilitate an easy and promptdisclosure.

7. Conclusion

It is indisputable that the FOI Act is an important tool for an accountable and transparent governance and democratic process. Research undertaken by the World Wide Governance Indicators Projects at the World Bank has observed that freedom of speech and the process of accountability that follows it, has a significant impact on the quality of governance of the country (The lawyers chronicle) .The citizens of Nigeria have the right to know how their government officials and the people they elected are handling their affairs. Nigeria, like many countries of the world have in 2011, enacted an Act to guarantee this right. What remains is the need for full implementation of the Act so that all and sundry, especially the media can bountifully harvest the benefits of the Act without fear. It is hoped that the observed challenges would be effectively taken care if the recommendation proffered in this paper are fullyimplemented.

8. References

1. 1. Afolayan A. (2012), A Critical Analysis of Freedom of Information Act in Nigeria. http://odinakadotnet.wordpress.com.
2. Duru I., and Ugbo G.O. (2014), The Nigerian Journalists' knowledge, Perception and use of the Freedom of Information (FOI) Law in Journalism Practice, *Journal of Media and Communication Practice*, vol. 6(1), pp. 1-10.
3. Harper S. (2005), Quoted in implementing Nigerian's Freedom of Information Act 2011–The Journey so far. r2nigeria.org>FOI-assessment-

reports. Accessed 10/12/15.

4. Ladan, A.S., FOI Act Opportunities and Challenges for Journalists.
5. Lawyers Chronicle, Defamation Law: A limitation on the freedom of expression in a Democratic Society. http://thelawyerschronicle.com/defamationlaw-a-limitation-on-freedom of information. Accessed16th of October 2016.
6. Lawyer's Chronicle,Information Gathering in Nigeria: Freedom of Information Act to the Rescue, Retrieved 24th of October 2015 http://the lawyerchronicle.com/information-act–to–therescue.
7. Mohammed, S. (2015), Much Ado about Freedom of Information Act www.Dailytrust.com.ng/dailyindexphp 155032 – accessed 15th October 2016.
8. Omu, F. R., (1978), Press and Politics in Nigeria, 1880- 1937 London: Longman.
9. Robert, A., (2000), Freedom of Information Act: Parliamentary of the United Kingdom. http://www.allafrica.com. Accessed 26th April 2016.
10. Udofa I. J., (2011), Right of Freedom of Expression and the Law of Defamation in Nigeria, *International Journal of Advanced Legal Studies and Governance*, vol. 2(l), pp. 75-84.
11. Ukunno, M., (2001), Reason for non- implementation of Freedom of Information Bill. The Punch Newspaper of 13thAugust 2010.
12. Yusuf A. I., SAN (2014) The Freedom of Information Act and the Challenges of the Practice of Journalist in Nigeria, *The Jurist*, vol. 19.

The Greek Regulatory Framework on Personal Data Protection with emphasis on Controller Obligations, following the Implementation of the Relative E.U. Directives

by Eugenia Alexandropoulou[1] & Maria Nikita[2]

1. Introduction

The Greek legal framework concerning personal data protection is derived from a) Law 2472/1997 [1][7] for the "Protection of Individuals with regard to the processing of personal data", through which the Directive 95/46/EC on "the protection of individuals with regard to the processing of personal data and the free movement of such data" has been implemented in Greek Law, b) Law 3471/2006 [9][13] for the «Protection of personal data and privacy in electronic communications including the amendment of Law 2472/1997", as amended, through which the Directive 2002/58/EC on "Privacy and Electronic Communications" and the Directive 2009/136/EC "amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws" have been implemented in Greek Law, c)the general legislation for the protection of personality [15], applied until the introduction of L.2472/1997.

1 Professor, Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece, e-mail: ealex@uom.gr.

2 PhD candidate, Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece, e-mail: nikitama@uom.gr.

The first part of this paper refers to the main obligations of the data processor, namely "the controller" (observing processing principles, obtaining the consent of the data subject and taking appropriate technical and organizational measures which includes secure data deletion). In the second part a test of legitimacy of personal data processing is suggested in order to establish whether data are lawfully processed by the controller. The third part deals with data subject rights and the fourth presents the Greek independent administrative Authorities who are responsible for the supervision of the implementation of the relative regulations. The paper ends with a Conclusion, which includes final thoughts and proposals for further research.

2. Obligations of the controller

These legal regulations, which are interpreted and implemented by the courts and the Hellenic Data Protection Authority, give rise to the obligations [3][4] of the data processor, namely "the controller". Violation of these obligations results in strict civil, criminal and administrative sanctions [8]. The main obligations of the controller are to observe the processing principles, to obtain the consent of the data subject, to notify (or obtain licence from) the Data Protection Authority and to take the appropriate technical and organizational measures for data protection. All these obligations which refer to "simple" and sensitive personal data [2][5] processing are dealt with below.

2.1 Observing processing principles

The key obligation of the controller is to observe certain processing principles which are included in the legislation for the protection of personal data namely: a) the legality of the purpose and means of processing, b) the proportionality, c) the accuracy of the stored data and d) the determined duration of the holding data [2] which, while it should be held in a form which permits the identification of the data subject, it has to be strictly for the period required to collect and process the data.

Of particular importance among these principles is the principle of proportionality, according to which the processing of personal data should be proportional to the purpose. For instance, in the field of e-communications, one of the consequences of the application of this principle is the

obligation of the controller to plan and choose the appropriate technical means, information systems and equipment for the provision of services by processing the smallest quantity of personal data required for the specific purpose. Another consequence of the application of the same principle is the obligation of the controller to include in the lists of subscribers available to the public, only such information as is absolutely necessary to identify a particular subscriber, i.e. a) for natural persons: name, surname, father's name and address and b) for legal persons: name or trade name, location, legal form and address. Any other components to be added require the consent of the data subject.

2.2 Obtaining the consent of the data subject

Another major obligation of the controller is to obtain the consent of the data subject. Consent must be free, explicit, specific and given only once the subject is fully informed. Moreover, consent can be either oral (for "simple" personal data) or written (for sensitive personal data). This obligation is subject to excemptions provided by the Law.

The data subject has the right to revoke consent at any time. If in the meantime the data have been disclosed to third parties, the parties in question must be informed of the revocation.

2.3 Notifying (or obtaining licence from) the Data Protection Authority

Another obligation of the controller is to notify the Data Protection Authority for simple data processing or to obtain licence from the above Authority for sensitive data processing. This obligation is subject to exemptions provided by the Law.

2.4 Taking appropriate technical and organizational measures

A particularly important obligation of the controller is to take appropriate technical and organizational measures to safeguard the security of the data processing. In the field of e-communications data protection, the law takes into consideration the financial interests of the controller and applies the principle of proportionality by stating that security measures must guarantee a level of security appropriate to the risk presented, including the state of art technology and the cost involved. Moreover, the controller is obliged to inform the subscribers of specific security dangers. Furthermore

the controller must not enter the users' terminal without their knowledge in order to access information, hidden information or trace the activities of the user by using spyware, web bugs, hidden identifiers or other similar devices. The use of such devices is permitted following user consent and only for legitimate purposes, such as special offers, the use of GPSs', weather forecast and traffic and tourist information.

2.5 Secure data deletion in a digital environment

Taking appropriate security measures also includes secure data deletion. According to Directive 1/2005 of the Hellenic Data Protection Authority, personal data must be destroyed by the controller when the purpose of the processing is completed. Moreover, personal data must be destroyed in such a way which makes it impossible for them to be recovered at any time in the future and by any means.

Bearing in mind that deleting a file does not erase it completely from the hard disk, the data may be recovered using special software tools. The reason for this is that when a file is created, a directory for that file is also created and when a file is deleted, only the reference of the file is deleted [16].

The most appropriate way to securely delete data that are stored in rewritable devices, like hard disks and DVDs, is to overwrite them. At this point, it is worth mentioning that government agencies have the capacity to recover data that have been overwritten as many as 21 times [16]. So, the more the data are overwritten, the less likely they are to be recovered.

There are many special software tools which secure the complete removal of data from rewritable devices by overwriting them several times. The software tools mentioned in the Directive 1/2005 are file erasers, file shredders and file pulverizes. These are advanced security tools which remove personal data from hard drives by overwriting them several times with carefully selected patterns or rewriting them several times with a random series of binary data.

Although these software tools make it impossible for data to be recovered using regular software, it might be possible through using computer forensic tools. Hence, in the case of highly sensitive data, the most effective way to delete them is to completely destroy the device on which they are written.

In case of violation of the security measures, strict civil, penal and administrative sanctions are imposed. For example, the Hellenic Authority

for Communication Security and Privacy imposed a fine of 100,000€ to a telecommunications service provider (Decision 74/2006) because it failed to take all the necessary security measures to prevent access to call subscribers data from unauthorized employees. Likewise, it imposed a fine of 76,000,000€ to a telecommunications service provider for 8 violations (Decision 5/2007) including the violation of the waiver of confidentiality, the use of illegal software, the lack of internal security measures and the failure to inform subscribers of the existing security risks and their consequences.

Moreover, DPA has also dealt with cases that concern the failure of banks and other private and public organizations to take adequate security measures. According to the decisions 11/2005, 12/2006, 13/2006, 14/2006, 15/2006, 16/2006, 17/2006, 18/2006, 12/2007, 13/2007, 14/2007, 15/2007, 21/2007, 55/2007, 71/2012, 73/2012, 76/2012, 129/2012, personal data were found exposed in waste bins not having been destroyed. The DPA gave them a formal warning to comply with the Directive 1/2005 and imposed fines proportional to the importance of the documents concerned.

3. Testing the legitimacy of personal data processing

In order to establish whether data are lawfully processed by the controller, the implementation of the following three steps test is suggested [2].

3.1 First step

Firstly, the application of the four operational principles must be examined. These are the principle of scope, of proportionality, of accuracy and of respect of storage time. If these principles have not been applied during data processing, then the processing is illegal. Consequently, there is no reason to continue to step 2 and the control terminates here.

3.2 Second step

Where all the above principles are applied, the data subject's consent is then required. If the data subject's consent is legally given, then data processing is legal and the control is completed.

3.3 Third step

On the other hand, where the data subject's consent does not exist, it must be investigated whether this is a special case and thereof an exception to

the rule and the subject's consent isn't necessary. If this is the case, then the processing is considered legal and the control is again completed.

4. Rights of the data subject

The Greek Regulatory Framework has established three basic rights [2][14] to protect the data subject when his personal data are processed. According to Law 2472/1997 the data subject has the right to information, to access and to objection. In particular, he has the right to be informed when his personal data are being processed. He can also have access to them and even raise an objection if the processing is illegal or the data are false.

The controller is obliged to respect the rights of the subject. Violation of these will again result in strict civil, penal and administrative sanctions [2].

4.1 Independent public authorities for data protection

The supervision of the implementation of the legal frameworks on personal data protection has been assigned to the Hellenic Data Protection Authority (D.P.A.). More specifically however, the supervision of e-communications protection has been assigned to the Hellenic Authority for Communication Security and Privacy (A.D.A.E.).

4.2 The Hellenic Data Protection Authority

The D.P.A. (www.dpa.gr) [6][10] was set up by article 15 of Law 2472/1997, following the guidelines set in the article 9A of the Greek Constitution. It reports to the Minister of Justice and is located in Athens. It is composed of seven members, a senior judicial officer (president), university professors and associate professors and experts in the field of data privacy.

The authority's responsibilities are administrative–supervisory and regulatory-advisory. Moreover, the D.P.A. issues decisions to solve differences between the data subject and the controller and has the right to impose administrative sanctions. The D.P.A., also, issues directives for the uniform implementation of regulations concerning the protection of individuals from the illegal processing of personal data, addresses recommendations and instructions to the controllers and gives opinions on any legal arrangement and policy privacy. Finally, the D.P.A. prepares annual reports on the implementation of its mission and cooperates with the relevant authorities of other Member States of the European Union and the Council of Europe.

4.3 The Hellenic Authority for Communication Security and Privacy

In order to protect the confidentiality of mailing, free correspondence or any other communication, as well as the security of networks and information, the Hellenic Authority for Communication Security and Privacy (A.D.A.E., www.adae.gr), mentioned above, was established (article 1 of law 3115/2003, following the guidelines set in paragraph 2 of the article 19 of the Greek Constitution). The concept of privacy encompasses the control of observing and regulating the terms and processes of the waiving of privacy as foreseen by the law.

The A.D.A.E. is an Authority with administrative independence, subject to parliamentary control. It is based in Athens but can function and set up office anywhere in Greece.

5. Conclusion

Following the relevant E.U. Directives, the Greek legislator has established a satisfactory legal framework to safeguard personal data protection. However, the «omnipresent» Information Society requires the constant vigilance of the legislator and its immediate response to the rapid development [11] of information technology.

In addition to the above, it is also accepted that the use of technology must be in such a way so as to ensure the constitutionally guaranteed personal data protection and not to violate privacy. To achieve this, not only is legislative contribution needed, but also the vigilance of computer scientists and data subjects [12].

Another major contribution is the cooperation of the data controllers. This contribution includes the adoption of self-regulation policies, which would go beyond the minimum legal protection.

Finally, looking to the future, further developments on the subject should concentrate on forming a general self-regulation policy, which can be adapted by organizations according to their specific needs.

6. References

1. Alexandropoulou-Egyptiadou, E., "Legal assurance of confidentiality

of mobile communications", Dikaio Meswn Enimerwsis kai Epikoinwnias (Information and communication media Law) - DiMEE, vol. 5, pp. 446-459, Oct. 2008. In Greek.

2. Alexandropoulou-Egyptiadou, E., Legal aspects of information technology, ed. A. N. Sakkoula, Athens-Komotini, 2007, Christodoulou,K., Personal Data law, ed. Nomiki Bibliothiki, Athens 2013. In Greek.
3. Alexandropoulou-Egyptiadou, E., Personal data - Legal framework of their e-processing, ed. A. N. Sakkoula, Athens-Komotini, 2007. In Greek.
4. Alexandropoulou, E., and Mavridis, I., "Personal data protection and use of R.F.I.D. Legal and technological approach", Harmenopoulos, vol. 61, pp. 493-504, April 2007.
5. Avgoustianaki, M., "Protection of individuals from the processing of personal data", Dikaiwmata tou Anthrwpou (Human Rights) - DtA, p. 673, Nov. 2001. In Greek.
6. Christodoulou, K., Protection of personality and contractual freedom in public utility networks, 1st ed., A. N. Sakkoula, Athens-Komotini, 2007, p. 111. In Greek.
7. Georgiadis, G., "The Law 3471/2006 for the protection of privacy in electronic communications", Chronika Idiotikou Dikaiou –ChrID, p. 17, January 2007. In Greek.
8. Gerontas, V., Protection of individuals with regard to the processing of personal data, 1st ed., A. N. Sakkoula, Athens-Komotini, 2002, p. 221. In Greek.
9. Igglezakis, I., Sensitive personal data, 1st ed., A. N. Sakkoula, Athens-Komotini, 2003, pp. 78-82. In Greek.
10. Kaisis, A., and Paraskevopoulos, N., Personal data protection, 1st ed., Sakkoula, Athens-Greece, 2001. In Greek.
11. Karakostas, I., "Protection of privacy in the information society", Proc. 1st Conference of the Scientific Council of the Information Society, Electronic Democracy - Information Society and Citizenship, Nov. 2003, p. 205. In Greek.
12. Katramados, D. "Individuals' protection from the processing of personal data (Law 2472/1997)", Dikaiwmata tou Anthrwpou (Human Rights)

- DtA, p. 577, March 1999. In Greek.

13. Mallery, J. R., "Secure file deletion: fact or fiction?", GSEC Practical Assignment, Version 1.2e, Dec. 2006.
14. Murakami, Y., "Privacy issues in the ubiquitous information society and law in Japan", Proc. IEEE International Conference on Systems, Man & Cybernetics: The Hague, Oct. 2004, vol.6, pp. 5645-5650, doi: 10.1109/ICSMC.2004.1401093.
15. Nikita, M., RFID in the Supply Chain and the Privacy Concerns, in Bottis, M., Alexandropoulou, E., Iglezakis, I., (edit.) Values and Freedoms in Modern Information Law & Ethics, Proceedings of the 4th International Conference of Information Law and Ethics, University of Macedonia, 20-22 May 2011, ed. Nomiki Bibliothiki Group, Athens 2012, pp. 1212-1233.
16. Nikita, M, RFID chips and EU e-passports: the end of privacy?, in Bottis, M., (edit.) Privacy and Surveillance-current aspects and future perspectives, Proceedings of the Liss-Cost seminar in Athens, Greece "Surveillance in Academia", 2012 plus selected papers from ICIL 2011 and 2012 in Corfu, Greece, ed. Nomiki Bibliothiki Group, pp. 199-229.
17. Nikita, M, The recommended RFID privacy and data protection impact assessment framework in the EU, in Bottis, M., Alexandropoulou, E., Iglezakis, I., (edit.) Lifting the barriers to empower the future of Information Law and Ethics, Proceedings of the 6th International Conference of Information Law and Ethics, University of Macedonia, 30-31 May 2014, ed. The University of Macedonia Press, Thessaloniki 2015, pp. 197-210.
18. Papakonstantinou, E., Information technology legal issues, 1st ed., Sakkoula, Athens-Komotini, 2006, p. 23. In Greek.

The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa? *

by Lukman Adebisi Abdulrauf ** *& Charles Manga Fombad* ***

1. Introduction

Globalisation and the increasing interdependence of states has led to the conclusion of a great number of treaties and other regional (and sub-regional) arrangements which regulate matters that had hitherto been regulated by national law.[4] This is especially so in subjects like data protection which require a great deal of harmonisation for effective implementation. Moreover, the need for free flow of information means data protection has increasingly become transnational in nature.

An efficient and effective data protection framework is very important because it will provide legal protection to individuals from the harm resulting from the manual or automated processing of their personal information.[5] The value of 'personal information', which is information that relates to or identifies (or is capable of identifying) a natural (or legal) person, is in its movement across borders. This raises legal issues regarding the protection of such information, which is considered 'sacred' because of its depic-

* This article was originally presented at the 7th International Conference on Information Law and Ethics (ICIL) held at the University of Pretoria, South Africa on 22-23 February 2016. We thank the conference organisers and participants. We also thank the reviewers for the insightful comments. All errors, however, remain ours.

** Centre for Human Rights, Faculty of Law, University of Pretoria, South Africa and Lecturer, Department of Public Law, Faculty of Law, University of Ilorin, Nigeria. E-mail: lukmanrauf@gmail.com

*** Professor of Law, Institute for International and Comparative Law in Africa, Faculty of Law, University of Pretoria, South Africa.

4 D. Sloss, 'Non-self-executing treaties: Exposing a constitutional fallacy' (2002) 36(1) *UC Davis Law Review* 1, 3.

5 A. Roos, 'Data protection' in D. Van der Merwe *et al. Information and communications technology law* (2008) 313. J. Neethling *et al. Law of personality* (LexisNexis, 2005) 267.

tion of one's personality, especially when its movement across various jurisdictions cannot be easily controlled. Admittedly, such issues are essentially domestic in nature. However, problems arise when personal information is to be transported to a jurisdiction without an efficient legal regime for its protection. It is in this kind of situations that regional initiatives, such as the African Union Convention on Cyberspace Security and Protection of Personal Data ('AU Convention' or 'the Convention')[6], becomes significant.

The controversy over whether (or not) data protection is a human right now seems to be more or less settled.[7] In fact, there are strong arguments that the right is now a *sui generis* right independent of privacy, although such arguments are yet to find a basis in Africa. Some scholars even argue that data protection has crystallised into a norm of customary international law.[8] All these depicts the importance of data protection to any human right system. It was a recognition of the importance of data protection that led the AU to adopt the Convention. However, this Convention has provoked mixed reactions from stakeholders and privacy advocates. While some are skeptical as to its effectiveness, others have welcomed it as a cause for celebration of human rights on the continent.

In view of the above, this paper interrogates whether the Convention may enhance the prospects for the protection of human rights in Africa. The analysis of the Convention in this paper will address two crucial issues. Firstly, whether the Convention is capable of attracting wide-scale adoption and implementation by state parties? To answer this question, the provisions of the Convention will be examined alongside long-standing data privacy instruments. In this respect, the substantive provisions of the AU Convention will be compared with the Council of Europe (CoE) Data Pro-

6 African Union Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV) available at https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (accessed 27 January 2016).

7 Especially in Europe. See generally G.G. Fuster, *The emergence of personal data as a fundamental right of the EU* (Springer, 2014). See also O. Lynskey, 'Deconstructing data protection: The 'added value' of a right to data protection in the EU legal order' (2014) 63(3) *International and Comparative Law Quarterly* 569.

8 For example, M. Zalnieriute, 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) 23(2) *International Journal of Law and Information Technology* 99.

tection Convention[9](and the EU Directive).[10] This is because, apart from the AU Convention, the CoE Convention is the only binding instrument on data protection as a matter of international law.[11] In fact, the CoE Convention is viewed 'as having potentially 'universal' application, i.e. proving the basis for global data protection standards.'[12] Thus, a discussion on the AU Convention alongside the older and more mature CoE Convention may be an important determinant of the quality of the former. The second issue to be investigated is the possible obstacles the Convention may face in the realisation of effective human rights protection in Africa.

The paper is organised in six parts. The second part examines the prospects for building the African information society and the challenges to human rights protection. Part three discusses subregional initiatives on data protection prior to the AU Convention. Part four makes an in-depth analysis of the substantive provisions of the AU Convention and compares this with the provisions of the CoE Convention (and sometimes, the EU Directive). Part five reflects on the various challenges to the AU Convention in effective human rights protection in Africa. Finally, part six concludes that paper with key recommendations onsuccessful implementation of the Convention.

2. Building the Information Society in Africa and the challenges to human rights protection

Africa is currently making strenuous efforts at various levels 'to build the

9 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108 at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm (accessed 27 January 2016).

10 The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard To the Processing of Personal Data and on the Free Movement of Such Data. Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:31995L0046 (accessed 27 January 2016).

11 P. De Hert & V. Papakonstantinou, 'Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency?' (2013) *I/S: A Journal of Law and Policy*271, 278.

12 Indeed, this is so because the CoE Convention has allowed non-member states to accede to it. See C. Kuner, 'An international legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law & Security Review* 307, 313.

information society'[13] so as to enable it to benefit from the on-going globalisation process taking place around the world.[14] This is partly also in recognition that 'information is a crucial economic and social resource' and 'electronic networks and information technology present a new venue for social economic and cultural activity, at both local and global levels.'[15] A credible information society goes hand in hand with economic and social development which Africa desperately needs. It is therefore no surprise that, scholars and policymakers have consistently acknowledged the importance of a viable information society for economic development across the continent.[16]

Two major features of the information society are the proliferation of information and communication technologies (ICTs) and the increase in demand for personal information by various entities.[17] Both features in many ways pose a challenge to human rights. For example, the demand for personal information aided by increasingly ubiquitous ICT infrastructure

13 The concept of 'information society' is an elusive concept without a precise meaning or definition. According to Hamelink, the concept of information society 'refers to the growing significance of information products (such as news, advertising, entertainment and scientific data) and information services (such as provided by the World Wide Web); the increasing volumes of information generated, collected, stored and made available; the essential role of information technology as the backbone of many social services and as the engine of economic productivity; and the input of information processing into transactions in trading and finance'. C.J. Hamelink, 'Human rights for the information society' in B. Girard & S.O. Siochrú, *Communicating in the information society* (United Nations Research Institute for Social Development, 2003) 122.

14 See initiatives like the African Information Society Initiative (AISI) and the Regional Action Plan on the Knowledge Economy (ARAPKE) both specifically mentioned in the AU Convention.

15 United Nations Economic Commission for Africa (UNECA) *Africa's Information Society Initiative: An Action Framework to Build Africa's Information and communication Infrastructure* available at http://www.uneca.org/cfm1996/pages/africas-information-society-initiative-action-framework-build-africas-information-and (accessed 26 January 2016).

16 For example, N.J. Udombana, 'The information society, poverty and development: An African Perspective' (2005) 18(1) *Revue québécoise de droit international* 75, 77. Unfortunately, the digital divide, which is 'the unequally access to ICTs by various communities', is a major obstacle to a credible information society in Africa. See also UNECA (n 15).

17 N. Moore 'The information society' in Y. Courrier (ed.) *World information* (1997) 271 (although, she referred to three characteristics of an information society).

facilitates information collection and use in a way that often leads to loss of control by individuals' over their personal data. This may amount to a violation of individuals' rights to privacy, dignity and personality, among others. Such violations are now becoming prevalent in Africa, especially in areas such as proliferation of the internet, national identity cards schemes, SIM card registration and surveillance technologies.

2.1 Proliferation of the Internet and online services

Building a credible information society depends on the availability and access to the internet. Indeed, 'internet penetration is growing exponentially in Africa.'[18] With an estimated population of above a billion (November 2015), Africa has more than three hundred (300) million internet users[19], thus, has about thirty percent internet penetration.[20] The increasing presence of the internet poses a fundamental threat to privacy. The increase in internet access also comes with proliferation of online and social networking services. Daily activities can be performed online with e-banking[21] and e-marketing services.[22] In this way, sensitive transactions are increasingly being conducted and important data stored on the internet in Africa. This situation may sometimes result in users not knowing who has access to their personal information, why their personal information is collected and what it is being used for. For example, direct marketers and online advertisers may harvest this personal information and exploit them for economic gains. Privacy and data protection has always been an issue when personal information is used without the consent and choice of the individual. A related problem with the rise in the use of the internet is identity theft. Identity theft is a category of cybercrime which involves using another person's

18 E. Tamarkin 'The AU's cybercrime response: A positive start, but substantial challenges ahead' (2015) 73 *Policy Brief* 1. Also available https://www.issafrica.org/uploads/PolBrief73_cybercrime.pdf (accessed 27 January 2016).

19 Internet World Stats 'Internet users in the world by regions November 2015' available at http://www.internetworldstats.com/stats.htm (accessed 27 January 2016).

20 *Ibid.*

21 See generally A. Harris et al. 'Privacy and security concerns associated with mobile money application in Africa' (2013) 8 *Washington Journal of Law, Technology & Arts* 245.

22 Tamarkin (n. 15).

personal information to obtain credit, loan etc. Even the AU notes that improvement in internet infrastructure is problematic as '[b]eing wired to the rest of the world means we are now within the perimeter of cybercrime, making the continent's information systems more vulnerable than ever before.'[23]

2.2 National identity cards schemes

Many African states are in the process of developing comprehensive identity (ID) card systems to facilitate easy identification of criminals and maintenance of law and order. Using modern ICTs, extensive databases of individuals' personal data, including sensitive and biometric data, are kept by the government. According to Banisar, '[t]he most common ICT privacy issue currently facing African nations is the development of new citizen identification systems, including identity cards and passports.'[24] This has serious implications for the right to privacy especially because there was, hitherto, no regional instrument holding states responsible for personal information in their possession. Besides, many of these ID systems are developed and operated by foreign companies.[25] For example, Nigeria is in the process of developing a comprehensive e-ID card scheme with the assistance of an American company, MasterCard which means there could be vast movement of personal information from Nigeria to the United States where the headquarters of MasterCard is situated.[26]

2.3 SIM Card registration exercise

Another avenue for the harvesting of personal information which is increasingly becoming prevalent in Africa is the subscriber identity module

23 AU 'INFOSOC: Division of information society' available at http://pages.au.int/infosoc/cybersecurity (accessed 27 January 2016).

24 D. Banisar, 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16(1) *East African Journal of Peace & Human Rights* 124,126.

25 *Ibid.*

26 J. Oguntimehin, 'Implications of Nigeria's National ID card' http://www.iafrikan.com/2014/09/30/nigeria-national-id-card/#sthash.aDBRkrnA.dpuf (accessed 27 January 2016).

(SIM) card registration schemes.[27] Many African countries have a mandatory requirement for SIM card registration without an enabling law in place.[28] This has serious data protection implications for the security of accumulated personal information. With sensitive personal information in the hands of the state, mobile surveillance is made easy with negative consequences for human rights.

2.4 Surveillance technologies

Surveillance technologies are now commonplace in digital age Africa. Surveillance, in this context, is a systematic means of personal information collection, especially by governments or private entities. States now have laws mandating telecommunication providers to integrate surveillance systems capable of interception of communications. For example, South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 requires service providers to incorporate surveillance machinery before they can offer services to the public.[29] Some African countries have even created more advanced means of surveillance. In Nigeria for example, there were reports that the government was in the process of developing advanced software to monitor internet communication.[30]

The above are some of the features of the African information society which is now characterised by 'massive data collection'. It is, perhaps, in recognition of 'information power' and the potential effects of its collection and use on human rights and fundamental freedoms that the AU Convention was adopted by African leaders. By this landmark Convention, member states of the AU reaffirm their 'commitment …to fundamental freedoms and human and peoples' rights' contained in various global and

27 A.B. Makulil, 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) *International Data Privacy Law* 163, 173-174.

28 Ibid.

29 See Banisar (n. 24) 129.

30 Ogala Emmanuel, 'EXCLUSIVE: Jonathan Awards $40 Million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians' *Premium Times*, April 25, 2013 available at http://bit.ly/12K1rUR (accessed 27 January 2016).

regional instruments.[31] Before the Convention, however, a number of important initiatives had been undertaken by regional economic communities (RECs) in Africa. Some of these initiatives will be briefly examined.

3. Regional and subregional initiatives on data protection prior to the AU Convention

Africa, though a relatively late entrant in the field of data protection, but it is making considerable efforts in the field. Developments in this area were heralded by a number of regional, sub-regional and domestic initiatives. Prior to the AU Convention, a number of African countries had introduced data protection laws in their legal systems. However, national legislation does not entirely deal with the issues that may arise when personal information crosses different borders.

Due to the limitations of national legislation in dealing with the matter, subregional initiatives therefore, become imperative. RECs were the subregional groupings that championed subregional initiatives. RECs in Africa were originally not established to 'foster human rights, but to facilitate a process of economic convergence through closer economic and financial cooperation and harmonisation policies and programmes.'[32] With time however, human rights became a critical aspect of their mandates.[33] With regard to data protection prior to the AU Convention, four RECs had taken concerted actions by adopting legal instruments to address the matter.[34]The Economic Community for West African States (ECOWAS) is the first subregional body to adopt a concrete framework on data protection law.[35] In 2010, it adopted the Supplementary Act A/SA.1/01/10 on Per-

31 See AU Convention, preamble.

32 F. Viljoen, *International Human Rights Law in Africa* (Oxford University Press, 2nd ed., 2012) 482.

33 As Viljoen argues, 'there is an obvious link between one of the main objectives of regional integration-improving the welfare of the people in the participating countries and the realization of socio-economic rights.' (n. 29) 482.

34 Although, the AU currently recognises only eight RECs.

35 A.B. Makulilo, 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review*78, 82.

sonal Data Protection within ECOWAS ('ECOWAS Supplementary Act').[36] According to Bygrave, the Act was the 'leading initiative' on data protection in Africa.[37] Greenleaf also contends that the Act spurred data protection laws in West Africa.[38] To make the Supplementary Act legally binding on member states, it is annexed to and forms an integral part of the ECOWAS Treaty.[39] Therefore, a violation of the Supplementary Act by member states can be enforced by the ECOWAS Court of Justice.[40] Being a supplementary Act, the ECOWAS treaty 'may be legally binding in creating substantive rights in countries where treaties have direct effect and do not require local enactment.'[41] Apart from its sectional application, the supplementary Act has been criticized for the fact that it does not provide clear sanction for a member state who fails to transpose the Act in its domestic laws.[42]

The East African Community (EAC) also developed a data protection framework-the EAC Legal Framework for Cyber Laws (Phase 1 & 2) 2008/2011.[43] Unlike the ECOWAS Supplementary Act, however, the legal framework is not binding on member states. It merely 'contains a series of recommendations made to the governments of partner states about reforming national laws to facilitate electronic commerce, to facilitate the use of data security mechanisms; to deter conduct designed to undermine the confidentiality, integrity and availability of information and communication technologies; to protect consumers in an online environment, and to

36 Adopted 16 Feb 2010. ECOWAS Supplementary Act available at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf (accessed 27 January 2016).

37 L. A. Bygrave, *Data privacy law: An international perspective* (Oxford University Press, 2014) 80.

38 G. Greenleaf, 'Sheherezade and the 101 data privacy laws: origins, significance and global trajectories' (2014) 23(1) *Journal of Law, Information and Science* 8, 22.

39 See ECOWAS Supplementary Act, art. 48.

40 Makulilo (n. 33) 83.

41 G. Greenleaf & M. Georges, 'African regional privacy instruments: Their effects on harmonization' (2014) 132 *Privacy Laws and Business International Report* 19.

42 Makulilo (n. 33) 87.

43 Draft EAC Legal framework for Cyberlaws (2008) available http://www.eac.int/index.php?option=com_docman&task=doc_view&gid=632&Itemid=148 (accessed 27 January 2016); Framework for Cyberlaws, Phase II (UNCTAD, 2011) http://r0.unctad.org/ecommerce/docs/EAC_Framework_PhaseII.pdf (accessed 27 January 2016).

protect individual privacy.'[44] Furthermore, the EAC legal framework was 'designed to harmonize the law reform process between the EAC Partner States, as well as reflecting international best practice.'[45] In this regard, paragraph 2.5 contains the recommendations on 'data protection and privacy'.[46] However, the frameworks 'do not provide any content principles as minimum standards for its members to adhere.'[47] This is, arguably, not a welcome development for the right to data protection which requires that certain minimum standards are specified for the processing of personal information.

The next significant subregional initiative prior the AU Convention is that of Southern African Development Community (SADC) with its Data Protection Model Law ('Model Law').[48] The objective of the Model Law, among others, is to 'create a uniform system in a given area in order to create a safe environment for citizens.'[49] Thus, the Model Law seeks to ensure harmonisation of data protection policies in member states. One of the factors that made this necessary was the permeability of traditional borders between countries. The model law gave prescriptive guidance to member states in enacting their data protection legislation. Like the EAC Framework, the SADC Model Law, of course, is not binding. This, therefore, limits any potential influence it may have in effective human rights protection in that region.

In 2013, the Economic Community of Central African States (ECCAS/CEMAC) made its own contribution to data protection in Africa by adopting a model law containing three texts on electronic transactions, data protection, and cybercrime. These texts were as draft directives.[50]

With these initiatives Africa has arguably become a 'home to some of

44 Draft EAC Legal framework for Cyberlaws (n. 40) 3.
45 Ibid.
46 Ibid, 17.
47 Makulilo (n. 33) 84.
48 Data Protection: Southern African Development Community (SADC) Model law https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf (accessed 27 January 2016).
49 Ibid, 3.
50 See Greenleaf and Georges (n. 38).

the most prescriptively ambitious data privacy initiatives at regional and sub-regional levels'.[51] Greenleaf and Georges assert that '[n]ow it is Africa that is leading global expansion' of data protection law. Notwithstanding this, the above initiatives cannot be considered to be credible substitutes for a *unified* continent-wide data protection initiative. This is because the wider the jurisdictional scope of a data protection instrument, the better the transboundary nature of data protection. On the other hand, harmonisation at the global level is considered by some to be like a mirage[52] because of the notoriously 'wide' and 'vague' conception of privacy in different parts of the world. Regional initiates, therefore, become the next point of call. Since the AU is making strides in human rights protection lately, it goes without saying that it was the proper institution to initiate reforms on data protection in Africa. It is on this basis that the AU's initiative – the AU Convention – deserves a detailed examination.

4. The AU Data Protection Convention

The AU set up, in the Constitutive Act and other instruments, Africa's regional system for promotion and protection of human rights.[53] This sets out not only to attain human rights objectives, but to use human rights-based means (or principles) to achieve those objectives.[54] As a key human right in the digital age, the role of the AU in data protection is vital – hence the Convention. This is perhaps the reason why Greenleaf and Georges describe the adoption of the Convention as 'potentially [the] most important development [on data protection] in Africa.'[55]

51 Bygrave (n. 34) 80.

52 See generally Kuner (n. 9) 307. C. Kuner, 'The European Union and the search for an international data protection framework' (2014) 2(1) *Groningen Journal of International Law* 55.

53 Viljoen (n. 29)152.

54 Ibid, 165.

55 G. Greenleaf & M. Georges 'The African Union's data protection Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws & Business International Report* 18-21.

4.1 Background to the AU Data Protection Convention

Before the adoption of the AU Convention, some efforts on data protection had been made by the AU. The first of such efforts was in 2011 with the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.[56] This draft was subsequently reviewed, albeit with a slight name change in 2013. The second draft was the African Union Convention on the Confidence and Security in Cyberspace.[57] These drafts were heavily criticised by the private sector, civil society organisations and privacy advocates because they had little involvement in the process.[58] In May 2014, there was a meeting of experts from the AU member states' ministry of justice to carry out a thorough review of the drafts.[59] On 27 June 2014, the AU Convention was adopted at the 23rd Ordinary session of the AU Summit in Malabo.[60] The reason for the slight change in name is still unclear. However, it is submitted that the present Convention is largely similar to the previous drafts.

The Convention has a broad scope to cover three important areas of cyber law: electronic transactions, data protection, cybersecurity protection/ cybercrime. This paper focuses on only the data protection provisions of the Convention.

4.1 Object and purpose of the Convention

Like most data protection instruments, the AU Convention has two broad objectives. Firstly, it commits state parties to 'establish a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data and to punish any violation of pri-

56 See http://au.int/en/cyberlegislation (accessed 27 June 2016).

57 Ibid.

58 E.P. Kenyanito, 'Africa moves towards a common cyber security legal framework' https://www.accessnow.org/africa-moves-towards-a-common-cyber-security-legal-framework/ (accessed 27 January 2016).

59 Ibid.

60 "Mixed feedback on the 'African Union Convention on Cyber Security and Personal Data Protection" available at https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html (accessed 27 January 2016).

vacy without prejudice to the principle of free flow of data.'[61] Secondly, the framework so established by member states shall ensure that any form of data processing respects fundamental freedoms and human rights while recognising the right of the state, local communities and the purposes for which businesses were established.[62] The objectives of the Convention show an unequivocal human rights protection agenda. Furthermore, the Convention recognises the interests of other entities in individuals' information like states, local communities and the purpose for which businesses are established. It, therefore, enjoins member states to establish a framework to carefully balance these broad objectives.

The objective of the Convention contains certain obscure terms. The first is 'protection of physical data'. Obviously, the Convention seeks to protect personal data like all data protection instruments. However, questions could arise regarding whether 'personal data' has the same meaning as 'physical data'. Unfortunately, the latter term is not defined in the definition section of the Convention. It is arguable that both terms mean the same thing. Perhaps the AU Convention adopted the term to distinguish personal information of natural persons from that of legal persons, since only the former falls within its scope. Furthermore, the use of the term 'local communities' as part of the institutions with rights over personal information is obscure and the term is not also defined in the Convention.

Since the AU Convention is not intended to be self-executing, certain issues, based on lessons that can be drawn from Europe, must be taken into consideration by state parties when establishing their legal regimes on data protection. Firstly, the CoE Convention, in stating its primary role as a human rights instrument, provides that it seeks to 'secure in the territory of each party for *every individual, whatever his nationality or residence*, respect for his [or her] right and fundamental freedoms, and, in particular, his [or her] right to privacy.'[63] This provision 'is in accordance with the

61 AU Convention, art.. 8(1).

62 AU Convention, art. 8(2).

63 CoE Convention, art. 1. See also Consultative Committee (T-PD) 'Modernisation of Convention 108: Final Document T-PD (2012)' available at https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_E_Convention%20108%20modernised%20version.pdf (accessed 27 January 2016).

general principles of the CoE and its member states with regard to the protection of individual rights.'[64] Thus, 'clauses restricting data protection to a state's own nationals or legally resident aliens would be incompatible with the convention.'[65] The AU Convention has no similar provision hence, it is arguable that the Convention only commits state parties to establish legal frameworks applicable to only citizen of state parties.[66] Secondly, based on the objectives of the AU Convention (and the CoE Convention), securing the right to privacy is explicitly mentioned as a core objective. However, from recent jurisprudence of the EU and scholars' opinion, while privacy is at the heart of data protection, the latter serves a multiplicity of interest beyond privacy concerns.[67] Thus, the trend nowadays is for data protection instruments to avoid a provision stipulating that securing privacy is a core objective.[68]

The AU Convention, like the CoE Convention, explicitly states its primary role as a human right instrument.[69] This is important because of the growing debates regarding whether or not data protection is a human right due to its substantial affiliation to trade. Besides, scholars like Makulilo, ar-

64 Commentary on the provisions of the Convention in 'Data protection: Compilation of Council of Europe texts' available at https://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf (accessed 27 January 2016) 22.

65 Ibid.

66 Indeed, the Constitution of the Federal Republic of Nigeria, for example, has been described as being discriminatory as its Bill of Rights is only applicable to Nigeria citizens. A. Kusamotu, 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by Article 25 of European Union Directive 95/46' (2007) 16(2) *Information & Communications Technology Law* 149, 154.

67 Bygrave (n. 34) 119. In fact, Bygrave notes that 'in some respects, data privacy canvasses more than what are typically regarded as privacy concerns.'

68 See for example the Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data ('draft EU Regulation') which provides in art. (2) that 'This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.' Compare with EU Directive, art. 1(1) & CoE Convention, art. 1. The draft EU Regulation is available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 27 January 2016).

69 AU Convention, art. 8. See CoE Convention, art. 1 and Proposals for modernization of the CoE Convention (n. 60) art.. 1.

gue that African countries seem to have lost sight of the purpose for regulating data processing.[70] They mainly enact data protection legislation for trade benefits that will accrue to them from countries within the EU.

4.2 Scope and Application

The AU Convention is applicable to any *processing* carried out in the territory of a state party of the AU.[71] State parties of the AU here refer to all the fifty-four (54) African countries with the exception of Morocco.[72] The term processing is defined in article 1 of the Convention as 'any operation or set of operations which is performed upon personal data whether or not by automatic means'. A non-exhaustive list of such activities is stipulated.[73] The Convention, further, provides, again, that it applies to 'any collection, processing, transmission, storage or use of personal data by a natural person, the state, local communities, public or private corporate bodies.'[74] Outlining specific processing activities again in section 9 appears to be superfluous. Moreover, the trend among recent data protection regulations is no longer to distinguish between these stages, but to use a generic term 'processing' which is broad enough to cover all the stages.[75]

The definition of personal information is also important to the scope of the Convention. As Schwartz and Solove point out, the existence of personal information is a jurisdictional trigger to the application of data protection instruments.[76] The AU Convention defines personal data/informa-

70 Because of the Adequacy requirement of Article 25 of the EU Directive. A.B. Makulilo, '"One size fits all": Does Europe impose its data protection regime on Africa?'(2013) 7 *Datenschutz und Datensicherheit* 450.

71 AU Convention, art. 9(c).

72 It is based on this number that some commentators observe that 'The AU Convention has more potential state parties than any other international data protection agreement currently has ratifications. See Greenleaf & Georges (n. 52).

73 Such as processing for household activates etc.

74 AU Convention, art. 9.

75 A. Roos, 'Personal data protection in New Zealand: Lessons for South Africa (2008) 4 *Potchefstroom Electronic Law Journal* 62, 79.

76 P.M. Schwartz & D.J. Solove 'Reconciling personal information in the United States and European Union' (2014) 102 *California Law Review* 877, 879

tion[77] as 'information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.'[78] This definition is a substantial replication of the EU Directive.[79] The definition is wide enough to cover all information that identifies individuals, hence, member states can adopt the provision as it is in their legislation. It is also good for harmonisation purposes as a number of African countries have already adopted definitions, influenced by the EU Directive, in their laws.[80]

In addition, the Convention also applies to both automated and manual processing of data 'contained in or meant to be part of a file.'[81] By this provision, the AU Convention goes further than the CoE Convention as the latter only applies to automated processing of personal information.[82]

An innovation of the AU Convention with regard to scope is contained in article 9(d). This provision provides that the Convention places 'any processing of data relating to public security, defence, research, criminal prosecution or state security' within its scope. This is, however, subject to 'exceptions defined by specific provisions of other extant laws.'[83] The Convention, by this provision, as a general rule, requires that these processing activities must comply with the data processing obligations stipulated in section iii. This approach differs from the approach of the EU Directive[84]

77 Both will be used interchangeably in this paper.

78 AU Convention, art. 1.

79 See EU Directive, art. 2(b) of the EU.

80 For example, South African Protection of Personal Information Act (2013), art. 1 & Ghanaian Data Protection Act (2012), sec 96.

81 AU Convention, art. 1(b).

82 CoE Convention, art. 3(1) of the Convention. The CoE explains the rational in its explanatory report that 'Compared with manual files, automated files have a vastly superior storage capacity and offer possibilities for a much wider variety of transactions, which they can perform at high speed.' see para1 of the explanatory report to the Convention (n. 61) 19.

83 AU Convention, art. 9(d).

84 The EU Directive in art. 3(2) provides that it shall not apply to 'processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the

and answers of the numerous criticisms associated with excluding these processing activities outright. Usually, it is argued that excluding data processing for public security, defence,[and] criminal prosecution gives public/security agencies too much leeway with regards to individuals' personal information. The approach of the CoE Convention in article 9(2) is as well noteworthy, as it also prohibits derogations from the basic principles of data protection except if 'such derogations is provided for by the law of the party and constitutes a necessary measure in a democratic society' in the interest of public security and for the purpose of 'protecting the data subject or the right and freedom of others.'[85] Only the data security principle, however, admits of no derogation under the CoE Convention.

The AU Convention does not apply to data processing undertaken for 'personal or household activities.' This exception is also not absolute as it is further stipulated that 'provided… such data are not for systematic communication to third parties or for dissemination.'[86] Another aspect of data processing excluded from the scope of the Convention is 'temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary storage of data.'[87] This exception is unclear - it may be an instance of data processing which poses minimal risk based on the principle of *de minimis*. An observation with the provision on the scope of the Convention, which is indeed a welcome approach, is that it contains very few exceptions. This is an important protection against repressive African regimes who may want to rely on the Convention to provide sweeping exemptions thereby diminishing data protection in their countries.

Furthermore, it is arguable that the Convention does not apply to processing carried out for journalistic, research, literary or artistic purposes. This exception applies insofar as the processing is solely for journalistic, artistic and literary activity 'in accordance with the code of conduct of these professions.'[88] Personal information processing in this category are

activities of the State in areas of criminal law…'.

85 AU Convention, art. 9(2).

86 AU Convention, art. 9(2)(a).

87 AU Convention, art. 9(2)(b).

88 AU Convention, art. 14(3).

permitted so as to balance the potential conflict between data protection and freedom of expression.[89]

4.3 Fair information principles

At the heart of every data protection instrument is the fair information principles (FIPs). According to Bygrave, the principles 'denote the pith and basic thrust of a set of legal rules'.[90] In the AU Convention, the principles are contained in section III which is titled 'obligations relating to conditions governing personal data processing'. The Convention, unlike the European data protection instruments, set out the principles in a specific fashion which makes for easy reading and extraction by state parties. This is indeed a notable development in the Convention. The Convention contains six principles which could have been influenced by a combination of the Organization for Economic Cooperation and Development (OECD) Guidelines[91] and the EU Directives. The first principle is the 'principle of consent and legitimacy of personal data processing.' This principle is largely taken from the OECD Guidelines as the neither the CoE Convention nor the EU Directive makes consent a specific principle.[92] The AU Convention requires states to provide, in their domestic frameworks, that processing of personal data shall be legitimate if the data subject consents. Instances where the requirement of consent may be waived are also stipulated. These include cases of compliance with a legal obligation by the controller, performance of a public related task, performance of a contract which the data subject is a party and for the protection of the vital interest or fundamental right of

89 See generally EU Directive, art. 9.

90 L. A. Bygrave, *Data protection law: Approaching its rationale, logic and limits* (MIT Press, 2002), 57.

91 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 10 January 2016).

92 The proposal for modernisation of the CoE Convention takes note of the important place of consent and a specific section is dedicated to it. See Proposals for Modernisation (n. 61), art. 5(2) which provides that '[e]ach Party shall provide that data processing can be carried out on the basis of the free, specific, informed and [explicit, unambiguous] consent of the data subject or of some legitimate basis laid down by law…'

the data subject.[93] Consent of the data subject is defined as 'any manifestation of express, unequivocal, free, specific and informed will by which a data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subject to manual or electronic processing.' From this provision, the Convention requires member states to provide for an opt-in regime for consent rather that an opt-out consent. This is in line with current best practice in data protection regulations.[94]

Opt-in regime for consent appears to be in conflict with the legitimate interest of entities, like businesses, and may thus be problematic. This is more so that the Convention, unlike the EU Directive, does not provide for 'legitimate interest' ground to validate processing of other entities.[95] Thus, the AU Convention's provision for consent as the main legitimising factor for data processing by other entities may conflict with the rights of others. This may, therefore, question the human rights agenda of the Convention. The problem with the 'legitimate interest' ground for data processing is its extremely vague nature which makes it prone to abuse by businesses. It is, perhaps, in recognition of this fact that the AU Convention avoided 'legitimate interest' as an alternative to consent. Nevertheless, since the Convention states *ab initio* that the legal regime of member states should ensure that data processing 'respects the fundamental freedoms and rights of natural persons while recognising …*the purposes for which businesses were established*',[96] the interest of business must also be taken into consideration. Striking a balance between privacy rights of individuals' and interest of other entities is therefore required of the implementing authority.

The second principle is the 'principle of lawfulness and fairness of personal data processing.' In terms of the Convention, states parties are required to provide that processing of personal information 'shall be undertaken lawfully, fairly and non-fraudulently.' This principle is also contained in the CoE Convention.[97] The third principle is the 'principle of purpose,

93 AU Convention, art. 13. Principle 1.

94 See the draft EU Regulation, art. 4 on the definition of 'the data subject's consent.' See also Proposals for modernizing the CoE Convention, art. 5.

95 EU Directive, art. 7(f); Draft EU Regulation, art. 6(1)(f). See also Proposals for modernizing the CoE Convention, art. 5(2).

96 [emphasis added]. AU Convention, art. 8(2).

97 CoE Convention, art. 5(2).

relevance and storage of processed personal data'.[98] This principle applies mainly at the data collection stage of the processing cycle and it requires that 'data collection shall be undertaken for specific, explicit and legitimate purposes.' It is further provided that personal information must not be further processed in a way incompatible with the original purpose.[99] This principle is also contained in the CoE Convention.[100] The principle also contains the requirement that data collection shall be 'adequate, relevant and not excessive in relation to the purposes for which they were collected and further processed.'[101]

The fourth principle is the 'principle of accuracy of personal data.'[102] This principle requires that data collected shall be accurate and kept up to date where necessary. The Convention requires reasonable steps to be taken to 'erase or rectify' inadequate, incomplete processed personal information. This principle is also contained in the CoE Convention.[103] The fifth principle, the principle of transparency of personal data processing, is rather strange and vague. It requires data controllers to mandatorily disclose information on personal data. The Convention does not say who the data controller should disclose the information to. Is it the data subject or the National Protection Authority (NPA)? The principle is not contained in either the CoE Convention or the EU Directive. The recent reform process in European data protection regimes, however, shows the (possible) introduction of the principle. For example, the proposal for modernisation of the CoE Convention provides for the principle of 'transparency of processing' where state parties are required to see to it that the data controller ensures the transparency of data processing by informing the data subjects of 'the identity and habitual residence or establishment of the controller, the purposes of the processing carried out, the data processed, the recipients or categories of recipients of the personal data, and the means of exercising the rights set out in article 8, as well as any other information necessary to

98 AU Convention, art. 13 principle 3.
99 Ibid.
100 CoE Convention, art. 5(b).
101 This requirement is also a duplicate of the CoE Convention. See art. 5(c).
102 AU Convention, art. 13 principle 4.
103 CoE Convention, art. 5(d).

ensure fair and lawful data processing.'[104] Similarly, in the draft EU Regulation, the requirement of transparency is merged with the principle of fair and lawful processing where it is provided that personal information must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject.'[105] The transparency principle in the AU Conventionis most likely influenced by these developments and it is arguable that the principle was intended to operate in a like manner. This could, therefore, mean a possible introduction of a new norm in data protection law and its provision in the AU Convention is, indeed, a welcomed idea. However, it needs to be further explained in an explanatory memorandum.

The last principle is the principle of confidentiality and security of personal data processing where provision is made for processing of personal information to be carried out confidentially and in a protected manner, especially where the processing involves the transmission of the data over a network.[106] It is further provided that where the processing is carried out by a third party on behalf of a controller, the latter must choose a processor who provides sufficient guarantee and it is incumbent on the controller to ensure compliance with the security measures in the Convention. This principle is also contained in the CoE Convention.[107] There, it is an obligation on state parties to require that data controllers put in place appropriate security measures for the protection of personal information 'against accidental or unauthorized destruction or accidental loss… [and] unauthorized access'. The provision of the CoE Convention is more explicit than the AU Convention with regard to this principle. The proposals for modernisation of the CoE Convention makes an important addition to the security safeguard principle which is surprisingly missing in the AU Convention. This is a requirement of data breach notification where the controller must notify (at least) the supervisory authority of serious breaches.[108]

104 Proposals for modernisation of the CoE Convention, art. 7 bis on 'transparency of processing'.

105 (Emphasis added). See draft EU Regulation, art. 5(a). See also art. 11.

106 AU Convention, art. 13. Principle 6.

107 CoE Convention, art. 8.

108 See Proposals for modernization of CoE Convention, art. 7(b). This requirement is also contained in the draft EU Regulation but not among the FIPs. See draft EU Regulation, art. 31.

An important principle omitted in the AU Convention is the accountability principle. Accountability is an 'umbrella concept which covers a myriad of obligations'[109] and it commits a data controller to put in place the necessary mechanisms to ensure that all other principles are complied with. This principle is derived from the OECD Guidelines.[110] Van der Sloot argues also that it is implicitly contained in the draft EU Regulation.[111] The principle is neither contained in the EU Directive nor the CoE Convention. The absence of the principle in these key instruments is because it is embedded in other principles and obligations of the data controller and may therefore appear redundant to provide specifically for it.[112]

4.3.1 Sensitivity

Although some scholars choose to treat sensitivity as part of the principles,[113] we will discuss it separately here because of its significance in data protection law. The AU Convention, in article 14, provides that parties should prohibit any processing of sensitive data. Sensitive data is data 'revealing racial, ethnic, and regional origin, parental affiliations, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject'.[114] Sensitive data is further defined in article 1. A long list of exceptions is contained in the provision.[115] The categories of sensitive data provided under article 14 of the AU Convention, like its counterpart, the CoE Convention, appears to be closed. Both Conventions make it appear as if

109 B. Van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 307, 314.

110 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data para. 14. Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 27 January 2016). See also Asia Pacific Economic Cooperation (APEC) Privacy Framework, principle IX. Para. 26.

111 According to Van der Sloot, it is linked to the obligation of transparency in art. 22 of the draft EU Regulation. (n 106) 311.

112 For example, see AU Convention, art. 13, principle 6 para. (b).

113 See for example Bygrave (n. 34) 165 & Bygrave (n. 87) 68.

114 AU Convention, art. 14.

115 AU Convention, art. 14(2).

all the information listed in the respective provisions are the only category of information that may be considered sensitive.[116] The CoE Convention, in its explanatory report, however, maintains that the list is not meant to be exhaustive and a state party may add to it in its domestic legislation.[117] In any case, there is now a growing debate regarding the relevance of extra protection for a special category of personal information. De Hert and Papakonstantinou, for example, contend that processing intensive methods have blurred the distinction between sensitive and non-sensitive information.[118] Therefore, processing of an otherwise non-sensitive information (like meal preference) may lead to information that is considered sensitive (like religious belief). According to the CoE, 'the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which there are used.'[119] The CoE, however, went further to justify its continued inclusion in data protection instruments that 'there are [however] exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests.'[120]

4.3.2 Specific rights of data subjects and duties of data controllers

The AU Convention contains certain key rights of the data subject. These are the rights to information, access, object and rectification or erasure.[121] It has now become a tradition for data protection instruments to set out specific rights of data subjects, although the effects of these rights can still be gotten from the FIPs (which establishes obligations or duties of data controllers). For example, the right to information under the AU Convention in article 16 has the same effect as the principle of transparency of personal data processing (principle 5). The right to information requires data con-

116 Ignoring obviously modern-day sensitive information like information genetic data and biometric data.

117 Explanatory Report to the CoE Convention, para. 48.

118 P. De Hert & V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130, 133.

119 Explanatory Report to the CoE Convention, para 43.

120 Explanatory Report to the CoE Convention, para 43.

121 AU Convention, art. 16-19 respectively.

trollers to provide data subjects with some information like his or her (the data controller's) identity, the purpose of processing, the categories of data involved etc.[122] The approach may appear to be unnecessary since every duty bestows a corresponding right and *vice versa*. From this perspective, a 'right and duty are correlative and inseparable.'[123] There are no specific provisions on the rights of data subjects in the CoE Convention.[124] However, it was later inserted in the proposals for modernisation of the CoE Convention.[125] Certain rights are also separately provided for in the EU Directive and draft Regulation.[126] Since these influential data protection instruments have adopted this approach, it can be safely argued that the AU Convention, in this regard, is in harmony with international prescripts.

The Convention, furthermore, specifically outlines some obligations of a data controller. These obligations include confidentiality, security, storage and sustainability obligations.[127] In our view, highlighting these obligations again is unnecessary. This is because section III is a section which basically contains obligations of data controllers. The obligations contained in the AU Convention are largely influenced by the EU Directive.[128] The Directive, on the other hand, does not provide for some of these obligations in the section on principles/conditions of data processing.[129]

The obligation in article 23 of the AU Convention - sustainability obligations – is rather odd. It requires the data controller to take all appropriate measures to ensure that processed personal data can be utilised.[130] It further mandates the processing official to ensure that 'technological changes' are not an obstacle to utilisation of personal data. There is no similar provi-

122 AU Convention, art. 10. These rights seems to have been inspired by the EU Directive.
123 S.J. Charles Coppens, *A brief text-book of moral philosophy* (Literary Licensing, 1985).
124 However, the convention provides for some of these rights in art. 8 under 'Additional safeguards for the data subject.'
125 See art. 8 titled 'rights of a data subject'.
126 See EU Directive, arts 12 & 14. See draft EU Regulation, chap iii.
127 AU Convention, section V 'Obligations of the Personal data controller'.
128 AU Convention, section VIII.
129 For example, the 'confidentiality and security of processing' in section VIII of the EU Directive, are not contained in neither articles 6 nor 7 which contains the FIPs. In the AU Convention however, they are provided in principle 6 of art. 13 and repeated again in arts 20 and 21.
130 AU Convention, art. 23.

sion in other international data protection instruments which makes it the more confusing. The obligation is probably included in the AU Convention so as to re-emphasize the commitment of the AU member states to build a credible information society.[131] Thus, any obstacle to the free flow (and utilisation) of personal information, be it technical devices of the data controller, must be prevented. This obligation appears to be consistent with the objective of the AU Convention of protecting privacy 'without prejudice to the principle of free flow of data.'[132]

4.3.3 Data export regime

A fundamental objective of data protection law in general, and the AU Convention, in particular, is to ensure the free flow of information across borders.[133] This objective must, however, be reconciled with human rights and fundamental freedom of individuals. Personal information is exposed to the greatest risk in the process of exchange between countries. This is why it is now customary for data protection instruments to establish a special regime for data export. Article 14(6) of the AU Convention provides for rules on transborder data flows (TBDF). By the provision, a data controller is prohibited from transferring personal data to a non-member state of the AU except such a state guarantees 'adequate level of protection of privacy, freedoms and fundamental rights' of persons whose data are to be processed (transferred). This rule is, however, not applicable where the data controller requests authorisation from the NPA before the intended transfer.[134]

Certain issues arise with regard to the AU Convention's provision on-

131 See AU Convention, preamble.

132 In support of this view, Bygrave's comment on 'sustainability' in data protection laws seems relevant where he points out that '[d]ata privacy law has much the same aim and function as that policies of 'sustainable development' have in the field of environmental protection. Just as the latter policies seek to preserve the natural environment at the same time allow economic growth, data privacy law seeks to safeguard the privacy related interests of data subjects at the same time as it secures the legitimate interest of controllers in processing personal data.' See Bygrave (n. 34) 122.

133 For more on the importance of TBDF and the need for data protection, see L.A. Abdulrauf, 'Regulation transborder data flows for development in the G-77+ China: The role of data protection law' 31(1) *UNISA Latin American Report* (2015).

134 AU Convention, art. 14(6)(2).

this very vital rule. Firstly, regulation on data export is contained under the provision on sensitive data processing. This gives the impression that only sensitive data, as narrowly defined, is to benefit from this regime. The CoE Convention, for example, dedicates a whole provision for transborder data flow[135] and a protocol to supplement the provision.[136] Similarly, the EU Directive provides for TBDF in a whole chapter.[137] Another issue with the AU Convention's treatment of data export (or TBDF) is that the section is scanty. For example, the Convention provides that transfer can only be effected to non-member state with an adequate level of protection. What is considered adequate is not stated. Some commentators contend that it 'has a meaning informed by the usage of the same term by Article 25 of the European Union's data protection Directive.'[138] This view, however, amounts to too much speculation since the AU Convention operates in a totally different region. The CoE Convention also uses the term 'adequacy' without stating clearly what it means.[139] Greenleaf, therefore, argues that 'this is very similar to 'adequacy' in the context of the EU data protection Directive.'[140] This argument is plausible with regard to the CoE Convention rather than the AU Convention since the former largely operates in largely the same locality as the EU Directive. An obvious omission from the Convention is that it does not provide for an exception where information can be transferred to a non-member state without 'adequate' data protection

135 CoE Convention, art. 12.

136 See Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows'

137 EU Directive, chapter V.

138 Greenleaf & Georges (n. 52).

139 Addition Protocol to the CoE Convention, art. 2. But it is more logical to argue that the CoE will adopt the approach of the EU since they are both European institutions. 'Adequacy' as the criteria for transfer to non-state parties was replaced with 'appropriate' in the modernised convention. Greenleaf seriously criticised this replacement. According to him, there is a danger in replacing adequate with appropriate without an explanation as 'appropriate' has little or no meaning in the history of data protection law.' G Greenleaf, "Modernising data protection convention 108: A safe basis for a global privacy treaty" (2013) 29(4) *Computer Law & Security Review* 8.

140 Greenleaf (n. 136) 7.

regime. The CoE Convention[141] and the EU Directive[142] make exceptions where transfer can be effected in such a situation, especially where the data subject consents, for the legitimate interest of the data subject or if the data controller uses 'adequate' contractual clauses to safeguard such an information.[143] Such an omission has the effect of compromising the 'free flow of information' objective of the AU.

Admittedly, conventions usually do not make elaborate provisions so as to enable member states to make provisions for details in their legislation. However, leaving out important details will only jeopardise effective protection and complicate harmonisation efforts.

4.3.4 Oversight and enforcement in member states

According to Hustinx, data protection 'is special in the sense that it is considered to be in need of 'structural support' through the establishment of an independent authority with adequate powers and resources.'[144] The supervisory authorities are an element of effective protection of individuals with regard to the processing of their personal information.[145] Oversight and enforcement institutions will be particularly useful for African countries because data protection is a relatively new subject on the continent. There is therefore the need for dedicated institutions to interpret and administer the legislation. The AU Convention requires member states to establish institutional frameworks, NPA, to protect personal data.[146] The NPAs must be independent and ensure data processing is carried out in accordance with the Convention.[147]A very robust provision is made for the duties and powers of NPAs which include enforcement, education, auditing, issuance of codes and guidelines and participating in international negotiations.[148]

The AU Convention further requires that NPAs must establish mecha-

141 CoE Convention, art. 2(2)(b).
142 EU Directive, art. 26.
143 Makulilo (n 32) 88.
144 P. Hustinx, 'The role of data protection authorities' in S. Gutwirth *et al.* (eds.) *Reinventing data protection?* (Springer, 2009)133.
145 CoE Additional Protocol, preamble.
146 AU Convention, art. 11(1).
147 AU Convention, art. 11(1)(b).
148 AU Convention, art. 12(2).

nisms for cooperation with data protection authorities of third countries.[149] There is, however, no specific provision for NPAs of state parties to cooperate among themselves. The essence of a treaty of this nature is to promote harmonisation of laws and policies so as to enhance the free movement of personal information and advance the goal of building an information society in Africa. There is no better means of achieving greater harmonisation than by making provision for NPAs to cooperate among themselves. The CoE Convention specifically provides that 'supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties.'[150] This provision, without a doubt, fosters team work among member countries.

5. Some reflection on possible challenges of the AU Convention for effective human rights protection in Africa

The AU Convention contains far-reaching provisions on the protection of individuals with regard to the processing of their personal information. It shows that Africa, through the AU, is now coming to terms with the realities of the digital age by confronting head-on emerging human rights challenges. Notwithstanding this, there are a number of issues on effective realisation of the objectives of the Convention. These problems may be categorised into two–problems with the convention itself and other problems which are of a general nature.

5.1 Problems with regard to the Convention itself

With regard the Convention itself, there a number of issues. Firstly, it is extremely broad in scope. The Convention may be described as a 'package' which seeks to regulate Africa's most pressing problems in relation to ICTs. Thus, it is divided into three chapters–electronic transactions, data protection and cybersecurity. In essence, the Convention is a commercial at the same time, human rights and criminal law instrument. The regulation of these diverse subject matters in one legal document has implication for a

149 AU Convention, art. 12 (2)m.

150 Addition Protocol to the CoE Convention, art. 1(5). See also EU Directive, art. 28(6).

proper organisation of the document. For example, the provisionon direct marketing which is a crucial aspect of data protection law is placed in the chapter on electronic transactions.[151] Though, direct marketing is arguably a subject matter for both electronic transactions and data protection.

Another issue with this approach (of combining data protection with other instruments) adopted by the AU is the confusion that may arise when a state party is only interested in one of the subject matters regulated by the Convention. For example, can a state party ratify only the data protection aspect and leave out the rest? Or can a state party, after ratifying the Convention as a whole, decide to withdraw[152] from its obligations under a particular segment? Obviously, if a state does not want to be bound by certain provisions, the right way to go about it is by way of reservation. Unlike the CoE Convention, the AU Convention does not limit the right to making reservations.[153] Nevertheless, from the human rights perspective, combining the data protection with other subject matters, like e-commerce and cybercrime, is not a commendable approach. Besides, there is the possibility that so much attention will be placed on certain aspects at the expense of others. Since cybercrime is such a notorious phenomenon currently in Africa, it is likely that it gets most of the attention. For example, there are calls from some quarters that 'African states should focus on the convention's cybersecurity and cybercrime provisions first, as it is unrealistic to expect states to implement the entire convention in a timely manner.'[154] This is problematic for effective data protection in Africa.

A second problem with the Convention is that it contains a number ambiguous and archaic provisions. For example, it consistently uses the term 'local communities' without defining it. Similarly, article 10 on 'prelimi-

151 AU Convention, art. 4, Chapter 1.

152 Although, the Vienna Convention on the Law of Treaties (VCLT), in art. 56(1) provides that a treaty without provision on withdrawal is not subject to withdrawal. Nevertheless, the right to withdrawal may be may be implied from the provisions of the AU Convention, art. 38(4). Thus, this satisfies the provisions of art. 56(2) of the VCLT.

153 See CoE Convention, art. 25. However, international law scholars, like Viljoen argue that 'a boundless discretion [to enter reservation] could result in the absurd situation where a state ratifies a treaty, but then enters reservations to just every important aspect thereof.' (n. 32) 26.

154 Tamarkin (n. 19).

nary personal data processing formalities', requires that certain 'actions' are exempted from the 'preliminary formalities'. The question then is, what is preliminary formalities? Does it refer to steps that must be taken by a data controller before the commencement of processing? This seems to be the most logical interpretation of that provision taking into account the subsections in article 10 which make provision, *inter alia,* for declaration, notification and authorisation before processing. Article 10 (2) provides that a certain category of processing must be declared before the protection authority. Similarly, article 10(4) requires that certain processing must only be carried out after authorisation by the NPA. The question that arises in this regard is how can a NPA enforce these provisions in a world of increasingly complex and ubiquitous data processing activities characterized by Web 2.0 and cloud computing applications? Here also is an example of an archaic provision, as requiring declaration and notification for certain categories of processing may be practically impossible. Every processing activity could be easily monitored when data controllers are known and carry out processing in a definite environment which is far from the case today. It is perhaps in recognition of this fact that the reforms initiated by the EU is proposed replacing the notification requirement.[155] No such provision for notification is contained in the CoE treaty.

Furthermore, the Convention contains some inconsistencies. For example, the term personal data has been defined in article 1. However, in some cases, the Convention makes reference to 'electronic data'[156] or 'physical data'[157] or even 'computerized data'.[158] Unfortunately, the Convention, like many other African international instruments, does not contain an explanatory memorandum which may aid in the understanding of its provisions. On another level, there are a number of patent omissions from the Convention. For example, it does not contain a provision for data breach notification or privacy impact assessment. These are important features of modern-day data protection instruments. This is a reason why they are

155 De Hert & Papakonstantinou (n. 115) 139.
156 AU Convention, the preamble.
157 AU Convention, art. 8
158 AU Convention, art. 1

provided for in the reform process of the CoE Convention[159] and the EU Directive.[160]

Perhaps, the most serious problem of the Convention is the absence of a provision establishing a supervisory authority at the regional level. While the Convention requires member states to establish NPAs, there is no body linking their activities so as to ensure harmonisation (and increased cooperation) at the continental level. Article 32 of the Convention merely provides that the AU Commission Chairperson is responsible for implementing the Convention, but this cannot be a viable proposition for a regional data protection body because of the expertise needed. Both the CoE and EU have such a body. In the CoE Convention, a 'Consultative Committee' is established comprising of representatives of each state party.[161] The functions of the Committee include making proposals for facilitating and improving the Convention and expressing opinions on any questions regarding the application of the Convention.[162] Article 29 Working party plays a similar role under the EU Directive.[163] The AU may consider establishing a specific body for this purpose.

Some of the Convention's provisions are couched in a 'broad fashion' allowing member states to 'domesticate' or 'incorporate' in a manner that suits their local circumstances. This gives states some latitude to provide for specific details in their laws. It also 'helps battle obsolescence in the face of technological developments.'[164] However, there is a problem with this method especially in the African context. Firstly, it may undermine efforts at harmonisation and secondly, there is no strong obligation on states to ensure that the standard established by the Convention is the minimum

159 See proposals for modernization of the CoE Convention, art. 7(2).

160 See draft EU Regulation, arts. 31 & 32.

161 CoE Convention, art. 18(2).

162 CoE Convention, art. 18(3), in fact, the committee has been renamed as 'convention committee' and further strengthened in the proposals for modernization of the CoE Convention. See art. 19. See also Greenleaf (n. 136) 6.

163 See EU Directive, art. 29. It has also been replaced with a permanent European Data Protection Board and its powers has also been expanded in the draft EU Regulation. See arts 64-72. See also De Hert & Papakonstantinou (n 115) 141.

164 Comment made by Bygrave with regard to the modernization efforts of the CoE Convention. (n. 34) 40.

standard. The Convention merely requires NPAs to ensure data processing is consistent with the provisions of the Convention.[165] The implication is that state parties can enact data protection legislation with a far lower standard. The CoE Convention provides useful lessons in this regard. Article 11 encourages member states to provide 'a wider measure of protection' than that stipulated in the Convention. Thus, the principles in the CoE Convention 'constitutes only a basis on which states may build a more advanced system of protection.'[166] This is a useful lesson for the AU.

5.2 Other problems

Some other problems general may impede the smooth and expeditious realisation of the objectives of the Convention.

The first is the 'African problem' towards international (human rights) treaties. Ratification is the first problem in this respect. For example, the AU Convention has been adopted since June 2014. So far, no African state has ratified the Convention.[167] The Convention further complicates this 'African problem' by requiring at least fifteen (15) African countries to ratify it before it can come into force.[168] Attaining this number will not be easy which means it may take a very long time (possibly, years) before the Convention takes effect.[169] Even if the number of ratifications is attained, there are other hurdles. One such hurdle is that African states often ratify treaties without taking the necessary steps to implement them. Indeed, '[w]hen states ratify international human rights treaties, they undertake to domesticate and comply with their provisions.'[170] But such is rarely the case. The

165 AU Convention, art. 12(1).

166 Explanatory report to the CoE Convention, para. 61.

167 In fact, even the details of the Convention and its status list are yet to be uploaded on the AU website of treaties, conventions, and protocol. See http://www.au.int/en/treaties (accessed 27 January 2016).

168 Article 36 provides that 'This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.' This is Unlike the CoE which merely requires ratification by 5 countries to take effect. See CoE Convention, art. 22(2).

169 Indeed, history has shown attaining 15 ratifying States will be a huge challenge. See Vijoen (n. 29)156.

170 Viljoen (n. 29) 9.

dualist nature of the relationship between international and domestic law which prevails in many African states further complicates this problem. For an international treaty to have legal effect, such a treaty must not only be ratified but must also be domesticated (incorporated in law).[171] Without domestication, the AU Convention (unlike the ECOWAS Supplementary Act) is just like any other instrument since it is a non-self-executing treaty.[172] Thus, individual rights cannot be derived from it.

Besides the challenges of ratification and domestication (incorporation), another serious 'African problem' is compliance. Viljoen notes that 'the greatest challenge [in Africa] is to bring about compliance with the treaty provisions by government officials and nationals alike.'[173] Unfortunately, the Convention does not contain a provision providing sanctions for state parties who do not comply. Indeed, even the AU Constitutive Act 'is vague on enforcement and the imposition of sanctions in cases where states do not conform to AU norms.'[174] According to Makulilo, the lack of clear sanctions on member states who do not establish a framework will definitely undermine compliance level.[175] But then, Viljoen points out, quite rightly, that 'international legal norms only become truly effective if compliance is not motivated by coercion or self-interest, but flows from personal motivation brought about by an internal process of norm acceptance ('internalization').'[176]

A third problem which may be an obstacle to the AU Convention is the general African attitude towards privacy. The prevailing perception is that

171 Especially, common law countries for example Nigeria, based on sec 12 of the Constitution of the Federal Republic of Nigeria.

172 The treaty provides as an objective that 'Each state party shall commit itself to establishing a legal framework aimed…'. AU Convention, art. 8. Note that a non-self-executing treaty according to Vázquez, is "a treaty that may not be enforced in the courts without prior legislative 'implementation'." See C.M. Vázquez, 'The Four Doctrines of Self-Executing Treaties' (1995) 89 *The American Journal of International Law* 695. He relied on a host of US cases like *Frolova v. Union of Soviet Socialist Republics*, 761 F.2d 370, 373 (7th Cir. 1985); *Tel-Oren v. Libyan Arab Republic*, 726 F.2d 774, 808 (D.C. Cir. 1984).

173 (n. 29) 25.

174 Ibid, 165.

175 Makulilo (n 32) 87.

176 Viljoen (n 29) 25.

the concept of privacy is alien to Africa because of its communal orientation as against individualism which is perceived to be a Western idea.[177] Individualism goes with privacy and communalism is the antithesis. Even the African Charter on Human and Peoples' Rights (ACHPR) does not contain a right to privacy. In trying to rationalize the omission of privacy from the catalogue of rights in the ACHPR, Olinger *et al.* contend that 'privacy was simply not seen as a necessary right for Africans to live freely and peaceably.'[178] Another commentator contends that Africans generally suffer from 'privacy myopia' which means they underestimate the value of their personal data and the need for its protection.[179] Although scholars like Makulilo strongly reject the 'so-called' African conception of privacy, it must be admitted that privacy is still a largely underdeveloped concept in Africa. This will definitely have an effect on the implementation and compliance with the AU Convention. Many African leaders will not attach so much importance to the Convention and will prefer to rather focus on more contentious human rights issues. This may be a reason why there is as yet no ratification. Implementation of the Convention will definitely suffer because of the lack of political will.

The AU Convention will also have to compete with other data protection regimes. On the one hand, the EU Directive has been a major force in the adoption of data protection law in Africa.[180] Thus, African states prefer to adopt the EU-style data protection law so as to serve as a first step in satisfying the EU's adequacy requirement as contained in article 25 of the EU Directive. The EU's regime may, however, not be a problem *per se* since the AU Convention has basically similar provisions with the EU Directive. On

177 See L.A. Bygrave, 'Privacy and data protection in an international perspective' (2010) 56 *Scandinavian Studies in Law* 165-200. S. Gutwirth, *Privacy and the information age* (Rowman & Littlefield Publishers, 2002).

178 H.N. Olinger *et. al,*'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39 *The International Information & Library Review* 31, 37.

179 E.M. Bakibinga, 'Managing electronic privacy in the telecommunications sub-sector: The Ugandan Perspective' (2004) http://www.thepublicvoice.org/events/capetown04/bakibinga.doc (accessed 27 January 2016).

180 Makulilo (n. 67). See also M.D. Birnhack, 'The EU Data Protection Directive: An engine of a global regime' (2008) 24 *Computer Law & Security Report* 508-520.

the other hand, the AU Convention has to contend with regional data privacy instruments. African states tend to pay more allegiance to their subregional bodies than the AU. Rationalising the basis for this, Viljoen states:

> *The scale of the subregional is smaller than that of the continental level: it has greater geographic proximity, allowing for strategic closeness. It also has greater potential for trade links, increasing the immediacy of mutual incentives, presenting closer linguistic and cultural ties, and holding the promise of greater effectiveness in implementation and enforcement…*[181]

If subregional instruments provide for similar principles as the AU Convention, then, this will not be so much of a problem. The difficulty arises if a subregional instrument makes provision that conflict with those of the AU Convention. It is then that allegiance becomes an issue. While the AU Convention acknowledges existing instruments of RECs, its ability to bring their provisions in harmony with the Convention remains to be seen. Besides, some RECs, arguably, have relatively long-standing and more advanced data protection regimes than that of the AU Convention.[182]

The success of the Convention will very much depend on how well it is able to integrate and coordinate prior subregional and domestic initiatives on data protection. However, it would seem that 'integration on an Africa-wide scale is extremely ambitious' especially because of the population and size of the continent.[183] This will be the more difficult since there is an absence of a continent-wide normative standard for privacy in Africa's principal human right instrument, the ACHPR.

Finally, the tension between data protection and other human rights may also be a challenge to the effective implementation of the Convention. In this regard, the right to freedom of information (FOI)/access to information comes to light. Unlike the right to privacy, freedom of information is guaranteed and protected under the ACHPR.[184] In Africa today, there an intensive campaign by CSOs and others drive for states to adopt

181 Viljoen (n. 29) 470.
182 For example, ECOWAS.
183 Viljoen (n. 29) 471.
184 ACHPR art. 9.

and implement freedom of information legislation because of the strong desire for accountability of public office holders. Data protection is usually seen as antithetical to freedom of information since the former, in a way, restricts access to information while the latter promotes its free access. Thus, unlike data protection, freedom of information has attracted more attention from several actors which has led to its relative success on the continent. While both human rights seem conflicting, there are, in fact, meant to serve different objectives which should not create any tension.[185] Besides, both rights 'complement each other in holding governments accountable to individuals.'[186]

6. Conclusion: a reason to celebrate human rights in Africa?

2016 is a very significant year for human rights in Africa. According to the Vice-President of the African Court of Human and People's right in an address, '…2016 is a veritable watershed in the continental human rights trajectory: 2016 marks the 35th anniversary of the adoption of the African Charter in 1981; the 30th Anniversary of the entry into force of the African Charter in 1986; the 29th Anniversary of the operationalization of the commission in 1987… The year also marks the 10thAnniversary of the operationalization of the African Court.'[187] Because of the significance of 2016 to Africa, the international community will certainly pose some critical questions regarding the state of human rights. One such question is how human rights have fared in the face of relative advances in technology on the continent. Privacy and data protection will definitely attract more attention because of challenges that advances in technology pose to their effective

185 For more on the conflict between both human rights, see D. Banisar, 'The right to information and privacy: Balancing conflicting rights and managing conflicts' working paper, World Bank available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf (accessed 7 April 2016)

186 Ibid, 1.

187 Address by Hon. Justice Bernard M. Ngoepe, Vice President of the African Court on Human and Peoples' Rights, on the occasion of the Opening of the 55th Ordinary Session of the African available at http://www.achpr.org/sessions/55th/speeches/opening-statement-court/ (assessed 27 January 2016).

protection. The international community and relevant stakeholders will be interested in knowing what measures have been taken in advancing the right to privacy and data protection. Similarly, the international business community in particular, will want to know whether Africa is a safe destination for the transfer of personal data for business purposes. The state of privacy and data protection is therefore critical in establishing whether or not human rights can indeed be celebrated on the continent especially in this digital age and information society.

The initiative of African leaders through the AU in agreeing to this landmark Convention on data protection is definitely laudable. It shows that Africa is now ready to move a step further in human rights protection as part of its strong desire to build a credible information society. A number of important questions must, however, be answered to determine whether the Convention is a possible reason to celebrate human rights in Africa. Firstly, is the Convention in harmony with best practices on data protection? This question is significant because of the transboundary nature of information processing. It is therefore very important that the AU Convention is consistent with other influential data protection instruments. In this respect, the AU Convention can be celebrated as its provisions are, *prima facie*, a combination of the CoE Convention and EU Directive. Besides, it is provided in the Convention that its provisions 'shall not be interpreted in a manner that is inconsistent with the relevant principles of international law.'[188] Although it contains a number of ambiguous provisions, member states can extract its contents and incorporate it into their domestic legislation. Nevertheless, it is submitted that the provisions of the Convention must be used as a minimum standard in enacting data protection legislation by state parties.

Secondly, and most importantly, is the question of implementation and compliance. As earlier noted, ratification is not a problem *per* se in Africa, rather, implementation of (human rights) treaties is the big problem. This raises a lot of concern. The AU may face a particularly difficult challenge with regard to the implementation of the Convention because of the general attitude of Africans towards privacy related issues. The Convention further complicates the situation by giving states too much leeway towards

188 AU Convention, art. 33.

compliance with its provisions. Perhaps, this was done because of the weak conception of privacy on the continent. Thus, it was thought that there should be some latitude given to state parties to decide on implementation based on their local circumstances. If this state of affairs remain, the Convention will just be another human rights treaty which African countries merely ratify on paper without implementing.

African leaders need to understand that data protection is an imperative, therefore a necessary mechanism must be put in place to ensure that the Convention is not only domesticated but enforced. Governments have to appreciate that they have the responsibility to respect, protect, fulfil and promote human rights. These obligations apply equally to all human rights.[189] The AU must also, at the regional level, put in place appropriate mechanisms to ensure that parties not only ratify but strictly comply with their treaty obligations. Effective monitoring mechanism/agency must be established. This agency should adopt innovative mechanisms, such as state reporting and fact-finding missions, to ensure compliance. Furthermore, individual countries and RECs must ensure that their regimes are in harmony with the AU Convention. Since the AU is presumably the proper institution to set human rights standard on the continent, RECs' initiatives must be consistent with the AU Convention. This will go a long way in facilitating the easy flow of personal information within and across Africa. Similarly, a clear relationship must be established between the AU Convention and the RECs' initiatives. In this regard, the AU must ensure that the Convention plays a leading role in steering data protection on the continent. As such, regional (and domestic) initiatives must be consistent with the AU Convention. On the whole, the AU must appreciate that while building a credible information society is crucial for economic development on the continent, human rights protection is equally important and should take precedence.

On the whole, as the AU adopted this Convention shows that data protection is, at least, recognised as crucial. On this basis, human rights may be celebrated in Africa. However, much more needs to be done by the AU for the international community to take Africa seriously.

189 Vijoen (n. 29) 6.

Data Protection in an Emerging Digital Economy: The Case of Nigerian Communications Commission: Regulation without Predictability?

by Aaron Olaniyi Salau[1]

1. Introduction

Against the background of an astronomically rising telecommunications industry, this introductory section sets the scene for the rest of the paper. It catalogues the dividends of liberalisation of digital telecommunications, and outlines the basis of credible regulation of the telecommunications industry in Nigeria.

Africa's mobile telephony industry is witnessing tremendous growth, thanks to the wave of deregulation and privatisation of the telecommunications subsector that swept across the continent since the early 1990s.[2] Nigeria joined this trend in 1992, and has become Africa's largest mobile telecommunications sector.[3] Full liberalisation took root in early 2000 through the formulation and implementation of the National Communications Policy 2000. Complete re-organisation and transformation of the sector came about with the enactment of the Nigeria Communications Act 2003[4] ('the NCA 2003') which made the Nigerian Communications Commission (NCC) the sole and independent regulator of the Communications industry. The Nigerian Telecommunications Act No. 75 of 1992, which established the Nigerian Communications Commission (NCC) was repealed, while enunciation of National Communications policy 2000 to-

1 PhD Candidate, Department of Public Law, Faculty of Law, University of Cape Town, South Africa.

2 N. Jentzsch, Implications of mandatory registration of mobile phone users in Africa Telecommunications Policy, (2012) 36, pp. 608–620 at 1.

3 C. B. Opata, Regulatory Accountability in the Nigerian Telecommunications Sector (2013) 57 *JAL*, pp. 283–309.

4 Act No. 19 of 2003 published in Federal Republic of Nigeria Official Gazette no. 62, vol. 90 (Government Notice No. 115) of 19th August, 2003.

gether with the NCA 2003 opened up the sector to influx of foreign capital and local private investments.

Telecoms sector deregulation in Africa has generated rapid diffusion of mobile information and communication technologies (MICT) and spin-off services like online marketing and internet banking.[5] According to the international Telecommunications Union (ITU) forecast, Africa is expected to witness the strongest growth in mobile cellular phones by the end of 2014.[6] As at January 2016, Nigeria had a total of 151,357,769 active subscribers divided into mobile (GSM) lines: 149,022,919; mobile (CDMA) lines: 2,147,982 and fixed wired/wireless lines: 186,868[7] (though the total figure for connected lines is not yet available due to the ongoing SIM card registration). As at December 2014, GSM lines accounted for 98.30% of total telephony market, the Mobile CDMA lines 9.36% while the Fixed Wired/Wireless segment had a paltry 0.14%.[8] The new lease of life brought to Nigerians by improving telecommunications infrastructure and expanding access to services testifies to the gains and market potentials unlocked by deregulation. The NCC has licensed a national carrier - Globacom Nigeria Limited (GLO) – and three other long distance GSM operators – MTN, Airtel (formerly Econet) Nigeria Limited and MTS (Etisalat). Excepting GLO, the other three multinational companies. These companies and numerous others provide various telecoms, internet and ICT-related services. The unparalleled foreign investments in mobile telephone networks and telephone-related services has resulted into massive ownership and use of mobile handsets.[9] The availability of low-cost hand-sets coupled with af-

5 J. Aker and IMbitiMobile, Phones and Economic Development in Africa (2010) 24 *Journal of Economic Perspectives,* pp. 207-32.

6 See ITU "The World in 2014, ICT Facts and Figures", online: ICT <http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf> (accessed 15 January 2016).

7 NCC 'Subscriber Statistics' available at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73 (accessed 28 March 2016).

8 The Nigerian Telecommunications Commission *2014 Year End Subscriber/Network Data Report For Telecommunications Operating Companies in Nigeria* NCC Statistics-Annual_Industry_Statistics_Report_2014.pdf 1 (accessed 28 March 2016).

9 Ibid. Facts and figures available in NCC publications and website depict similar multiplier effects of regulatory action taken in the industry from 2001 to 2015 on job em-

fordable access tariffs have further enabled remotely located rural dwellers, the poor and low income earners to connect locally and internationally with far flung urban-based populations in real time.

Industry reform has brought multiplier effects not only on the telecommunications industry but the entire Nigerian economy in terms of overall investments, trades and services such that the telecoms subsector has been contributing an average of 8 percent per annum to Nigeria's overall Gross Domestic Product (GDP) since 2000.[10] A combination of market liberalisation, competition and economies of scale have led to a lowering of access costs and lifted barriers to mobile interconnectivity through introduction of innovative billing tariff plans. The ubiquitous nature of mobile telephony and the social services provided by production, advertisement, distribution and wholesale marketing of recharge cards, mobile hand-sets and vending of subscriber identification module (SIM) cards[11] for multiple mobile networks have created job opportunities for hitherto unemployed rural and urban poor. The value-added services associated with mobile telephony like internet connectivity provided by mobile phone companies and licensed internet service providers (ISPs) have created rapid expansion of internet services using Wi-Fi technologies.[12] Nigeria is also a budding market for 'smart phones' enabled for convergence of voice and data services. All of these make Nigeria's telecoms industry an emerging powerhouse in the African digitalized mobile telephone services.

This quantum leap did not come without some structural changes. It came about due to lenient national deregulation policies and the growing independent regulation of telecommunication services. The establishment of clear framework for independent regulation of the Nigerian telecommunications industry wasin itself part of an adaptation to a global policy

ployment opportunities, community development and other communication-related activities.

10 Ibid.

11 This is the card issued by mobile phone operators which provides the individual user with the appropriate number recognized by that network which a subscriber inserts into a mobile phone to access the mobile phone network. See 'SIM Registration' available at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=122&Itemid=113.

12 ITU op citn 5 19.

shift from state-owned monopolies towards market competition in the last quarter of a century.[13]

According to the ITU, a basic prerequisite for credible and stable regulation of the telecommunications industry is the existence of a clear legislative framework, and also, the capacity and professional ability of the industry regulator.[14] Indeed, Nigeria had been commended for adopting 'a clear policy for the development of the telecommunication sector, supported with a flexible regulatory framework'the major policy thrust of which was the economic regulation of the telecommunications sector.[15] The NCC was established as a semi-autonomous regulatory body within the ambit of overarching objectives of the National Telecommunication Policy 2000, which is 'national socio-economic development and seamless national integration into global communication networks in an efficient, affordable and reliable manner.[16] For the NCC therefore, as stated above, the legal and policy frameworks consist of the Telegraphy Act 1990[17], the NCA2003 and the National Telecommunications Policy 2000.[18] The NCC's regulatory mandate empowers it to engage in a great number of activities. These, among others, are to specify and publish technical codes and specifications[19]; prepare or require licensees or a designated industry body to prepare consumer codes[20]; determine, administer, monitor and enforce compliance with competition and anti-competition laws[21] on market dom-

13 C. B. Opata, op cit n 2, p. 283.

14 Ibid at 9 and 21.

15 Ibid at 3.

16 Ibidat 12.

17 No. 31 1998.

18 The primary function of the NCC includes the promotion of investments and private sector participation; the facilitation of entry into the industry and healthy competition among operators; implementation of standards and monitoring of operators for efficient and qualitative service; expansion of the nation's communication facilities; ensuring universal access to affordable telecommunications service for all Nigerians; management of the Universal Access Fund and protection of consumers. See s 4*(a)-(w)* of the NCA 2003; the Telegraphy Act No. 31 of 1998 and the National Telecommunications Policy 2000.

19 NCA 2003, s. 130(1).

20 NCA 2003, s. 106(1)(2)(3)*(a)(b)(c)*(4)*(a)(b)(c)(d)(e)(f)*(5)(6).

21 NCA 2003, ss. and 91.

ination[22] and interconnection[23] and ensure universal access for unserved, underserved areas and underserved groups[24]. Aside from technical conformity with the law, it can be argued that for consistency and predictability, these extensive rule-making powers, other functions of the Commission and objectives of the NCA 2003 must be exercised in the public interest and with regard for openness and consultations with stakeholders including the general public. The NCC has seized upon the broad mandate of 'economic and technical regulation' of the industry granted by the NCA 2003[25] and other enabling Acts to establish innovative licenses and prescribe conditions relating thereto. The NCC has crafted regulations on interconnectivity and consumer protection and lately, established subscriber information registration procedures to activate SIM cards.

However, the success story of digitised telecommunications in Africa is being marred by rising wave of mobile-phone related criminality culminating in the introduction of SIM card registration policies in most African countries[26] including Nigeria.[27] As in other many other African countries, the downside of Nigeria's telecoms industry successes is the ascription of rising wave of criminality to the widespread availability of unregistered SIM cards. According to interactions between security agencies and the NCC, the increasing difficulty of apprehending kidnappers who demand ransom from their victims' families through mobile phones, and resolving other phone-related crimes is fast becoming a security nightmare. This anonymity advantage of unregistered SIM cards seems to be attractive to criminals. Despite lack of data or research conclusively connecting availability of unregistered SIMs to increased kidnappings, the NCC seemed

22 NCA 2003, s. 90.

23 NCA 2003, ss. 96 and 97.

24 NCA 2003, s. 112.

25 NCA 2003, s. 2(1)*(w)*.

26 K. P. Donovan and A. K. Martin, The rise of African SIM registration: The emerging dynamics of regulatory change *First Monday*, vol. 19, no. 2-3, February 2014. Available at http://www.firstmonday.dk/ojs/index.php/fm/article/view/4351/3820. doi: http://dx.doi.org/10.5210/fm.v19i2.4351.

27 See the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 S. I. No. 35 published in Government Notice No. 229 Federal Republic of Nigeria Official Gazette No. 101 of 7th November, 2011 vol. 98 (hereinafter referred to as 'the NCC Regulations').

to have bowed to pressure to introduce a SIM card registration policy. The NCC Regulations effective from 2011 provides for mandatory biometrics data capture and registration of personal information of mobile phone subscribers. But before probing further the utility of the Regulations, the next subsection delves into standards of protection afforded by international data protection laws.

2. Data protection rationale and privacy standards

Technological convergence, globalisation, diffusion of intrusive technologies and interconnectedness of national telecommunication networks have made data security more imperative. The risks to individual rights inherent in fast dissemination, automatic processing and transfer of information at unimaginable speed by modern digital telecommunication services have always made them attractive for state regulation. Data protection laws therefore focus on data processing, which is the automated or manualcollection, registration, storage, use or dissemination of personal information.[28] Personal data has also been defined as the information that can be used to identify a natural individual.[29] The information can relate to a person's personal details, gender, health status, personal relationships, telephone calls, internet activities, banking transactions, etc. As such, data protection laws provide legal cover to the individual against misuse, misappropriation or unlawful disclosure of her personal information. The right to privacy uphold values such as dignity, autonomy and personality, which also underlie data protection, hence, most privacy laws often harbor data protection principles.[30] However, a conceptual clarification between data

28 A. Roos, "Data protection" in D. Van der Merwe et al., (2008) *Information and Communications Technology Law*, p. 313.

29 L. A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", 6 *International Journal of Law and Information Technology,* pp. 249-268.

30 A few examples from Australia are: the Privacy Amendment (Private Sector) Act 2000 (Cth); Privacy and Personal Information Protection Act 1998 (NSW); Information Act 2002 (NT); Information Privacy Act 2000 (Vic); Health Records (Privacy and Access) Act 1997 (ACT); Health Records and Information Privacy Act 2002 (NSW); Personal Information Protection Act 2004 (Tas); Health Records Act 2001 (Vic); Recommendations for introducing information privacy legislation in Western Australia: Office of the Attorney-General for Western Australia, Privacy Legislation for Western Australia

protection and privacy is beneficial. This clarification better serves human dignity because, as it was rightly observed, 'the latter serves a multiplicity of interest beyond privacy concerns'.[31] Based on the understanding that the right to privacy is a pillar of data protection, the following sections respectively engage with the concept of privacy, and the ethical foundations for data protection under international law, European standards and African prescriptions. The overall aim is to determine what these regimes offer as safeguards against misuse of telephone subscribers' information.

2.1 Defining privacy

Definitions of privacy vary widely according to context and environment. Components of privacy are wide reaching and extend to ability to protect one's bodily integrity, physical zones of intimacy[32] and informational about oneself.[33] The emphasis here is given to informational privacy. This idea of privacy posits that certain spheres of intimate individual activities involving personal information are inviolable and protected from monitoring by the State or other individuals and through secret surveillance. For example, Mill posits that 'there is a circle around every individual human being, which no government… ought to be permitted to overstep …'[34]. According to Alan Westin, privacy is the ability to control the information others have about you.[35] In accordance with the above philosophical views, it is an affront to one's privacy for an unauthorised opening, to read, divulge or record a person's a person's email and internet activities or eavesdrop on her conversations without permission or lawful excuse. It is also unlawful to appropriate or misappropriate another person's information for

Policy Research Paper (2003) referred to by David Lindsay An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law (2005), *Melb. U. L. Rev.*, p. 1.

31 L. A. Bygrave, *Data privacy law: An international perspective* (2014), p. 119.

32 S. Warren and L. Brandeis, The Right to Privacy (1890) 4 *Harvard Law Review,* p. 193.

33 D. Solove, The Origins and Growth of Information Privacy Law (2003) 748 *PLI,* pp. 53-6.

34 J. S. Mill, *Principles of Political Economy with some of their Applications to Social Philosophy (*1965), p. 938.

35 A. R. Miller, *The Assault on Privacy: Computers, Databank and Dossiers* 1971 at 25; A Westin, *Privacy and Freedom* 1 ed 1967 7.

commercial purposes without permission. Privacy exist in terms of 'ability to control the information others may have about you', to restrict physical access to oneself and limit access to intimate sensitive information about oneself.[36] This is so for several reasons; control over one's privacy enhances the sense of one's dignity and self-worth; it enhances the development of individual personality without manipulations by others while a sense of personal autonomy enables individuals create and maintain different social relationships.[37] In many countries, the concept has been fused with data protection, which interprets privacy in terms of managing personal information.[38]

2.1.1. The right to privacy in international law

The right to privacy is enshrined in standard-setting human rights instruments like the Universal Declaration 1948, art. 12[39], the International Covenant 1966, art. 17[40] and other international human rights instruments[41], several soft laws and Declarations. The International Covenant[42], art. 17 provides as follows:

1. No one may be subjected to arbitrary or unlawful interference with

36 O. O. Salami, Privacy Protection for Mobile Health (Mhealth) in Nigeria: A Consideration of The EU Regime for Data Protection as a Conceptual Model for Reforming Nigeria's Privacy Legislation. Submitted in partial fulfilment of the requirements for the degree of Master of Laws at Dalhousie University Halifax, Nova Scotia April, 2015, pp. 21-25.

37 Ibid at pp. 25-27.

38 D. Banisar and S. Davies, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments (1999) 18 *John Marshall Journal of Computer and Information Law*, p. 1.

39 G. A. res. 217 A(III), U.N. Doc. A/810 at 71 (1948).

40 G. A. res. 2200A (XXI), 21 U. N. GAOR Supp. (No. 16) at 52, U. N. Doc. A/6316 (1966), 999 U. N. T. S. 171, entered into force March 23, 1976.

41 Article 11 of the American Convention on Human Rights, Nov, 22, 1969, O. A. S. Treaty Series No. 36, at 1, OAE/Ser. L./V/II.23 doc. Rev. 2, entered into force July 18, 1978; the European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8 213 U. N. T. S. 222, entered into force Sept. 3, 1953.

42 The Covenant has been ratified by the greatest number of states. See Office of the United Nations High Commissioner for Human Rights, Status of Ratifications of the Principal International Human Rights Treaties as of 16 June 2006. Available at http://www.ohchr.org/english/bodies/docs/RatificationStatus.pdf.

his privacy, family, home or correspondence nor to unlawful attacks upon his honour and reputation.
2. Everyone has a right to the protection of the law against such interference or attacks.

The provision has been interpreted by the Human Rights Committee, the International Covenant's oversight body, in its General Comment 16 as a source of data protection principles applicable to both public and private entities.[43] According to the HRC:

> *The competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. … The gathering and holding of personal information on computers, data banks and other devices whether by public bodies or private individuals, and bodies must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.*

The HRC's Comment also covered the right of every person (or data subject) to have access to information held of them by public authorities and to correct whatever errors contained therein.[44]

However, the problem with HRC's General Comments is that they are not binding on States though they are authoritative expositions of the International Covenant.[45] Even citizens of States that have ratified the First Optional Protocol to the International Covenant may only bring complaints against such States before the HRC after exhausting all domestic remedies. Most importantly, the case law developed on art 17 reflect, but do not measure up to data protection principles as stated in international instruments such as the CoE Convention on data transfer and EU Directive

43 General Comment 18, issued 23.3.1988 (Un Doc A/43/40, 181-183; UN Doc CCPR/C/21/Add.6; UN Doc/HRI/GEN/1/Rev 1 21-23), paras. 7 & 10.

44 Ibid.

45 The International Covenant, art. 40(4).

on Data Protection.[46]

Nevertheless, veritable data protection principles are also deducible from the common agreement of states under art. 2(2) of the International Covenant whereby a State-party 'undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant'. The article enjoins each state Party to the present Covenant undertakes to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant. This presupposes a positive obligation on States. Furthermore, a progressive understanding of the nature of rights within the United Nations is that the International Covenant imposes obligations on States to take concrete steps including through legislation to protect, respect and fulfil human rights.[47] Within this new conception, the States must *respect* (not interfere with), but also *protect* (put measures in place to prevent and remedy infringements of) and *fulfil* data privacy rights.

2.2 The normative basis for data protection

The normative basis for data protection principles is found in various international and regional standard-setting human rights treaties dealing with the right to privacy such as the Universal Declaration of Human Rights 1948 (The Universal Declaration)[48] and the International Covenant on Civil and Political Rights 1966 (The International Covenant).[49] African countries too are beginning to pay more attention to data protection. By adopting the Convention on Cyberspace Security and Protection of Personal Data 2014 ('the CCSPPD')[50] the African Union signified its preparedness to promote

46 Bygrave, n. 28, p. 258.

47 Vienna Declaration and Programme of Action, adopted by the World Conference on Human Rights in Vienna on 25 June 1993. Available at http://www.ohchr.org/Documents/ProfessionalInterest/vienna.pdf (assessed 29 March 2016).

48 Universal Declaration op cit n 38.

49 International Covenant op cit n 39.

50 African Union Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV) available at https://ccdcoe.org/sites/default/files/documents/AU-

an information society. TheCouncil of Europe (CoE) Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the Free Movement of Such Data 1981 (Council of Europe 1981)[51], the European Community's (EC) Directive on Data Protection[52], Privacy of Electronic Communications Directive (EU 2002/58/EC)[53] and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data Convention 1981 (OECD 1981)[54] are some of the extant regimes. The basic essence of data protection principles stated in the CoE Convention, the EU Data Directive as well as laws emanating from them is to protect fundamental rights notably right to privacy[55]. Nigeria is signatory to the Universal Declaration, International Covenant (except its Optional Protocol) and the AU CCSPPD though it is yet to ratify any of them. This, however, does not detract from Nigeria's obligations to respect, protect and fulfil its international human rights obligations as dictated by the Vienna Convention on Human Rights.[56] Similarly, Nigeria is not bound by the European standards. There is however an emerging trend to comply with EU prescriptions of transboundary movement of personal data in terms of interconnectivity arrangements[57]. In recent times, the NCC has

270614-CSConvention.pdf (accessed 24 March 2016).

51 ETS No 108 adopted 28.1.1981, entered into force 1.10.1985, hereinafter the CoE Convention.

52 Directive/95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ No L 281, 23.11.1995, 31), adopted 24.10.1995.

53 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (as further amended) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (accessed 29 March 2016). This Directive repeals the Telecommunications Data Protection Directive (97/66/EC) and obligates telecommunications companies, within the context ofprocessing personal data to take extra measures against nuisance calls and protect confidentiality of communications and anonymity rights of callers.

54 Hereinafter 'OECD Guidelines 1981'.

55 See arts 1 of the CoE 1981 and EU Data Directive 1994.

56 Op cit n 46.

57 C. B. Opata, Transplantation and Evolution of Legal Regulation of Interconnection

also looked towards Europe in fashioning anti-market domination[58] and interconnectivity rules.[59] The growing influence of the European Union Data Protection Directives in technologically advanced countries[60] including emerging data protection regimes in Africa[61] has also been observed. Moreover, global interconnectivity of telecommunication networks makes possible transfer of subscribers' personal information beyond the shores of Nigeria a foregone conclusion. It would therefore not be out of place to consider Europe's standards in this paper.

2.2.1. European data protection principles

The discussion here focuses on principles sifted from major European data protection regimes mentioned above. Data protection laws first emerged in Germany before spreading across Europe and other parts of the world due to concerns for abuses inherent in digital transmission of personal information made possible by automated information and communication technologies.[62] Hence, Europe has one of the most well developed and up to date data protection regimes.[63]

Data protection principles in Europe are now fairly well established and prescribe general standards of protection for handling and processing of personal information by data controllers, processors and also in specific industries.[64] The principles require that personal data must be:

Arrangements in the Nigerian Telecommunications Sector (2011) 14 *Int'l J. Comm. L. &Pol'y,* pp. 1-36.

58 C. B. Opata, Looking Towards Europe: Regulation of Dominance in Nigerian Telecommunications (2013) 14 *Competition and Regulation in Network Industries,* pp. 338-364.

59 NCA 2003, ss pp. 96-100.

60 G. Greenleaf, The influence of European data privacy standards outside Europe: implications for globalization of Convention (2012) 2 *International Data Privacy Law,* pp. 68-92.

61 A. B. Makulilo Data Protection Regimes in Africa: too far from the European 'adequacy' standard? (2013) 2 *International Data Privacy Law,* pp. 42-48.

62 D. Banisar, op cit, n 37.

63 O. O. Salami op cit n 35.

64 For example the EU Privacy of Electronic Communications Directives 2002/2/EC and 2002/58/ECapplyspecifically to processing of personal data in electronic communications services.

1. obtained fairly and lawfully;
2. adequate, relevant and not excessive to purpose of collection;
3. used only for the original specified purpose;
4. accurate and up to date;
5. accessible to the subject;
6. kept secure; and
7. destroyed after its purpose is completed.[65]

Bygrave[66] made a summary of data protection principles. Bygrave's summary correlate with Banisar and Davies' respectively as 'fair collection principle', 'minimality principle', 'purpose identification principle' and 'use limitation principle', 'data quality principle', 'individual participation principle' and 'security principle'.[67] Bygrave does not mention the 'destroyed after its purpose is completed' principle, but says every agency carrying out data processing must bear legal responsibility for every use to which data collected is put(accountability principle).[68]

The EU data protection model is based on 'enforceability', which ensures that data protection principles are enshrined in explicit laws and there is an independent entity styled 'Privacy Commissioner' to protect data subject's rights. But it can be argued that predictability is a function of enforceability, which ensure that rules accessible, serve legitimate interests and are compatible with aims of a democratic society (not subject to whims and caprices of data controllers). The EU Privacy of Electronic Communications Directive 2002, for example, regulates unsolicited direct marketing to all forms of electronic communications, unsolicited commercial (spam) and sms's to mobile telephones and provides a right of recourse in the event of unlawful processing. It also guarantees the right to withhold permission to use data in some circumstances.[69] The Directive ensures privacy of communications and internet use and that communication details are

65 D. Banisar, op cit, n 37, p. 11.
66 Bygrave, op cit, n 28.
67 Ibid.
68 Ibid.
69 F. Fakinsuyi, Nigerian Cyber Crime and Privacy Legislation, Time for Review (2010) 8 (downloaded from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1663633 on 29 March 2016).

deleted once calls are terminated.The wide acceptance of the CoE Convention 1981, EU Data Directive 1995 and EU Telecommunications Directive 1997 (repealed by theDirective 2002/21/EC) in the Eurozone has spurred other countries' adoption of data protection laws in line with the European model. However, how privacy rights are limited in the European Union have been more extensively discussed in literature on art 8 of European Convention on Fundamental Freedoms and Human Rights.[70]

2.2.2 The African model of data privacy

Not surprisingly, the AU CSSPPD – though a more expansive instrument – has borrowed significantly from the European model. But at the same time is commendable for underscoring African communitarian values in data protection strategies. However, the AU CSSPPD has not come into effect having not been ratified or domesticated by any African country.[71]

70 A comparison of art 8, ECHR and art 17 of international covenant reveals that art 8, which deals right to privacy in the European context is more explicitly worded than art 17. Art 8 provides thus:
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
The EU 'telephone interception cases' are the highlight the gist of art. 8(2). A summary of jurisprudence of the European Commission and European Court of Human Rights on art. 8(2) especially as regards the 'telephone interception cases' is that in limited circumstances the right to privacy protects a person's access to personal data held by public authorities. Moreover, enforcement of art. 8 is carried out by the European Court of Human Rights (ECtHR) whose judgements are legally binding on all signatories to the ECHR. Similarly, art. 10(1) also, in narrowly construed circumstances, recognises the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use data in some circumstances. See Bygrave, op cit n. 28.

71 A comparative analysis of the AU CSSPPD and the EU data protection principles have been expertly carried out by L. A. Abdulrauf & C. M. Fombad African Union Data Protection Convention 2014: A possible cause for celebration of human rights in Africa? Paper delivered at the 2016 ICIL Conference held at Pretoria, South Africa on 22-23 February 2016 (paper on file with writer).

3. Data protection in Nigerian law and the NCC regulations

This section problematises the Nigerian Constitution's underdeveloped state of legal protection for data privacy and engages with objectives underpinning the Nigerian SIM card registration policy ('the NCC Regulations') vis-à-vis the public interest in data protection. It argues that the fledgling safeguards in the NCC Regulations relating to phone subscribers' biometrics and personal data processing are weak, and offer little protection to privacy and other subscribers' rights in terms of recognized international standards. The adequacy of the Regulations is considered in light of some of the basic principles of data protection recognised above.[72]

3.1. Right to data privacy and the Constitution of the Federal Republic of Nigeria 1999

Nigeria is yet to enact a substantive or sectoral data protection law. To prepaid mobile phone subscribers in Nigeria as elsewhere, privacy, dignity and autonomy are crucial issues, hence the concern here is to ensure that adequate safeguards exist against potential abuses inherent in the application of the NCC Regulations. Few attempts to secure the much needed data protection rights of Nigerians can be found in the NCC's General Consumer Code of Practice for Telecommunications Services made pursuant to the Consumer Code of Practice Regulations in accordance with powers granted by s 21 of the NCA 2003.[73] The Code provides some protection for subscriber data collected by telecommunication companies. Essentially, these are broad and very limited efforts to protect the privacy of Nigerians (Salami 4). A Computer Security and Critical Infrastructure Protection Bill 2005 and Cybersecurity and Information Protection Agency Bill 2008 are currently considered by the national legislature.[74] The Nigerian Constitution guarantees the right to privacy under which the right to data

72 However, the extent to which prepaid SIM cards owners are entitled to anonymity from commercial advertisers and unsolicited contacts remains largely under-researched in literature and is not considered in detail in this paper.

73 The Nigerian Communications Commission Consumer Code of Practice Regulations 2006, Schedule 1 (as may be amended from time to time).

74 F. Fakinsuyi, op cit n 68, pp. 12-17.

protection may be subsumed.Section 37 of the Constitution of the Federal Republic of Nigerian 1999[75] (the 1999 Constitution) which guarantees the right to privacy[76] provides as follows:

> *The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.*[77]

This constitutional provision encompasses freedoms of communication and of information, vital to a democracy, and secures those rights to Nigerians, but not necessarily foreigners. The right to privacy is probably one of the most under-researched, under-litigated and under-developed rights in the Nigerian Constitution. The few instances in which recourse has been had to the right has been health-related cases. The instances involve the right of HIV-infected persons not to be discriminated against,[78] the duty of doctors not to disclose HIV status of infected clients to their sex partners[79] and the right of patents to informed consent.[80] The Nigerian Constitution is the yardstick for validity and operation of all other laws including international law, statutory provisions, rules of common law and equity.[81] In view of paucity of constitutional jurisprudence on data protection, a person may seek recourse to delict or common law torts of 'negligence', 'trespass to property', 'breach of confidentiality' or 'nervous shock' as a substitute for

75 Cap. C23 Laws of the Federation of Nigeria 2004. It came into effect on 29 May 1999. As discussed above, data protection principles may be found under the freedom of expression provisions (s 39), but is not explored further in this article.

76 Privacy rights are also embedded in other human rights provisions of the Nigerian Constitution namely, right to freedom of religion (s 38) and freedom of expression (s 39), but the discussion focuses on s 37–right to privacy.

77 Data protection principles may be found under the freedom of expression provisions (s 39), but is not explored further in this article.

78 E. Durojaye, So sweet, so sour: A commentary on the Nigerian High Court's decision in Georgina Ahamefule v Imperial Hospital & Another relating to the rights of persons living with HIV (2013) 13 *AHRLJ,* pp. 464-480.

79 B. Odunsi, Should Caregivers Be Compelled to Disclose Patients' HIV Infection to the Patients' Sex Partners? (2007) 38 *Studies in Family Planning* , pp. 287-306.

80 Y. Z. Lawal, E. S. Garbal and M. O. Ogirima et al., The doctrine of informed consent in surgical practice (2011) 10 *Annals of African Medicine,* pp. 1-5.

81 See the Constitution of the Federal Republic of Nigeria 1999 Constitution, ss. 1 & 12.

breach of privacy. However, the problem with tort actions is that a claimant must prove damage to be entitled to monetary compensation. But not so for claim for breach of human rights where damage is presumed. Arguably, s 37 protects data subjects in terms similar to what obtains under art 8 of the ECHR,[82] but this is still a very rudimentary aspect of Nigerian law. The low level of technological development might be responsible for the lack of litigation of privacy rights in Nigeria, but as Nigeria is Africa's fastest growing telecommunications market, the situation can no longer be tolerated. The lack of adequate data protection in Nigeria was decried by Ayo Kusamotu, who wrote:

> *One finds that the National Information Technology Development Agency (NITDA, a sub-agency of the Nigerian Communications Commission, has developed a draft Nigerian Information Technology Policy, which was approved by the Nigerian Federal Executive Council in 2001. NITDA's IT Policy identifies some of its objectives as 'promot(ing) legislation (Bills and Acts) for the protection of on-line business transactions, privacy and security' and 'enhanc(ing) freedom and access to digital information at all levels while protecting personal privacy'. Until 2007, this remains a good intention insofar as privacy is concerned since, while a draft Cybercrime Act has been produced in Nigeria in 2003, no data protection legislation has been enacted in the approach favoured by EU 46/95 (footnotes omitted).*[83]

For the regulation of an industry with rapidly changing technology such as telecommunications to be predictable, there must be assurance of regularity by means of a law upholding full-fledged rights of stakeholders. Therefore the next section analyses the NCC Regulations and the effect of paucity of data protection principles in its operation.

82 A. Kusamotu Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by art. 25 of European Union Directive 95/46 (2007) 16 *Information & Communications Technology Law*, p. 155.

83 Ibid.

3.2. NCC regulations: objectives, content and context

Prior to the roll out of mobile lines in 2001, no regulations or contractual requirement existed mandating identity verification of prepaid ('pay-as-you-go') subscribers of mobile telecommunication services either at point of sale or SIM card activation. Mandatory Registration Regulations (NCC Regulations) were formalised in 2011 after a stakeholder consultative process. As explained on the NCC website, the move for registration of SIM card users started in 2008 when security agencies approached the headship of the NCC for assistance in resolving the problem of identifying persons implicated in phone-related crimes. Registration policy was initiated on March 28, 2011 after an official flag-off ceremony performed in Abuja by the NCC Executive Vice Chairman, Dr. Eugene Juwah. Two basic prongs of mandatory registration policy are to make planning data available provide for the industry regulator and to combat the upsurge of 419 scams, kidnapping-related offences and terrorist activities, e.tc. The NCC Regulations was actually signed on the third of November 2011 in terms of powers conferred on the Commission by section 70 of the NCA 2003 and all other powers enabling it in that behalf.

The Regulation itself lists four main objectives of SIM Registration namely,

1. To assist security agencies in resolving crimes and by extension to enhance the security of the state.
2. To facilitate the collation of data by the Commission about phone usage in Nigeria.
3. To enable operators to have a predictable profile about the users in their networks.
4. To enable the commission to effectively implement other value added services like Number Portability among others.[84]

Though SIM card registration officially ended in 2012 mobile operators are still expected to continue registering new subscribers who will only be able to make emergency calls unless registered.

84 Nigerian Communications Commission 'Sim Registration' available on NCC website at http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=122&Itemid=113 (accessed 12 January 2016).

3.2.1. Data capture and creation of a central database

The Regulations call for creation of a central database for central processing of subscribers "personal information" including full names, date of birth and gender, occupation and "biometric information"-finger prints and facial image of all subscribers - which have been registered as provided under s. 11. The Database shall be segregated across network services so as to facilitate easy access persons authorised by the NCC.[85] Though it is to contain information compiled at network providers' own cost, the Central Database shall be the sole property of the Government of Nigeria.[86] The Regulations do recognize that the sheer number of existing subscriber may necessitate the use of independent contractors. Hence, 'data controllers' such as the Commission and network providers could employ an independent registration agent to carry out subscriber registration.[87]

3.2.2. Retention of information

The Regulations provides that a licensee 'shall have the right to retain and use its subscribers information on its network in accordance with the provisions of Part VI of the General Consumer Code of Practice for Telecommunications Services and any other instrument issued from time to time by the Commission'.[88] It also contemplates a potential request for access to the central database or general request for information by the national security adviser and security agencies in the normal course of crime investigation. In this respect, s. 8(1) provides that:

> *Notwithstanding the provisions of these Regulations restricting access to Subscriber Information on the Central Database and subject to the provisions of any Act of the National Assembly, subscriber information on the Central Database shall be provided only to Security Agencies; provided that a prior written request is received by the Commission from an official of the requesting Security Agency who is not below the rank of an Assistant Commissioner of Police or a co-ordinate rank*

85 NCC Regulations, s. 4(3).
86 NCC Regulations, s. 5(1).
87 NCC Regulations, s. 9(3)(4).
88 NCC Regulations, s. 7.

in any other Security Agency. (2) The written notice by the Security Agency pursuant to sub-regulation (1) of this regulation shall indicate the rank of the official of the requesting Security Agency and the purpose for which the information is required.

3.2.3. Privacy rights and safeguards against misuse of subscriber information

Certain provisions of the Regulations are very crucial provision in these regards. Section 9(1) is particularly pertinent because they recognised 37 of the Nigerian Constitution as the source of data protection rules. The section says that:

In furtherance of the rights guaranteed by section 37 of the Constitution of the Federal Republic of Nigeria, 1999 and subject to any guidelines issued by the Commission including terms and conditions that may from time to time be issued either by the Commission or a licensee, any subscriber whose personal information is stored in the Central Database or a licensee's database, shall be entitled to view the said information and to request updates and amendments thereto. (2) The subscriber information contained in the Central Database shall be held on a strictly confidential basis and no person or entity shall be allowed access to any subscriber information on the Central Database except as provided in these Regulations.

Section 7 allows a licensed operator to retain and use subscriber information as may be permitted by the Commission, but sections 9 and 10 further enjoin licensees, independent registration agents and subscriber registration solution providers, and the Commission, when applicable to:

i. retain refrain from retaining, duplicating, dealing in or making copies of any subscriber information or storing it in any form or for any purpose other than as stipulated by the Regulations or an Act of the National Assembly;
ii. take independent action and all reasonable precautions pursuant to international best practices to preserve the integrity or unauthorised disclosure of subscriber information in the course of capturing or processing the information;
iii. utilise personal information retained solely pursuant to the Regu-

lations, their operations, in accordance with the provisions of the General Consumer Code of Practice for Telecommunications Services, other instruments of the Commission and any Act of the National Assembly relating to use of personal information;

iv. not retain subscriber Biometrics after its transmission to the Central Database;
v. not release personal information to any person in breach of the Constitution or any other Act of the National Assembly;
vi. not release personal information subscribers to any third party, except security agencies,without obtaining the subscribers' prior written consent;
vii. not transfer any subscriber information outside Nigeria without the prior written consent of the Commission.

3.2.4. Penalties

The Regulations creates various offences and prescribes penalties for breaches of its provisions. For example, unlawful duplication, retention or dealing with subscriber information is an offence and attracts a penalty of N200, 000 (equivalent of $1000 US Dollars) per subscription medium.[89] Similarly, an entity that is 'found to have utilised a subscriber's information in any business, commercial or other transactions' is liable to a penalty of N1,000,000.00 (equivalent of $5000 US Dollars) per subscription medium.

3.3. Problems associated with the NCC Regulations

The right to privacy and data protection principles are not absolute. Data protection laws may exempt government and private organisations from strict compliance with informational privacy for overriding public interests such as public safety, national security, the rights and freedom of others, crime control. Also, in a sales of SIM card purchase agreement, a person may not have a reasonable expectation of privacy where he or she has 'ticked a box' authorising the use of his or her personal details for commercial purposes. International law interplays between data protection and its exceptions. Restrictions must not be unlawful, unreasonable or arbitrary,

89 NCC Regulations, s. 21(1).

but must be necessary in a democratic society and serve a legitimate purpose. It can be argued that limitation of data privacy must be within strict bounds of necessity and proportionality.

The potential adverse effects of SIM card registration schemes in Africa raises a number of questions including the question of the alleged link between crimes and use of mobile telephony.[90] The anonymity previously enjoyed by mobile telephone users in Africa has been increasingly eroded since 2006, due to adoption of mandatory registration of SIM cards by majority of industry regulators and governments in African countries including Nigeria.[91] The common argument in Africa and elsewhere[92] by proponents of registration is that criminals seeking anonymity are likely to use unregistered prepaid SIM cards. The counter argument, including available research evidence in Nigeria,[93] that such crimes are perpetrated by only a handful of people-sophisticated criminal networks - is equally plausible.

Mandatory registration directives and regulations usually provide for the processing – which involves the recording, storage and transmission - of raw personal data and information of subscribers. A sampling of mandatory registration procedures in three African countries, South Africa, Nigeria and the DR Congo conducted by Jentzsch is instructive.[94] It reveals that subscriber identity module (SIM) card owners must supply certain information including their full names, proof of physical address, date of birth, residential address, residency status and means of identificationto

90 I. Kerr 'On the identity trail: Understanding the importance and impact of anonymity and authentication in a networked society'. Retrieved September 2007, from http://www.idtrail.org/; K. Wallace, (1999) 1 *Anonymity, Ethics and Information Technology*, pp. 23-35.

91 N. Jentzsch, Implications of mandatory registration of mobile phone users in Africa, (2012) 36 *Telecommunications Policy*, p. 608.

92 See Government of Switzerland. (2003). Conventions des Nations Unies pour la répression du financement du terrorismeet des attentats terroristes à l'explosif. Retrieved July 10, 2007, from http://www.parlament.ch/afs/data/f/rb/f_rb_20020052.htm (Australian Communications Authority, 1997). Australian Communications Authority. (1997, December 22). ACA makes rule applying to pre-paid mobile services (Media Release No. 42 of 1997). Retrieved January 2016, from http://aca.gov .au/aca-home/media-releases/media_enquiries/1997/index.htm .

93 F. Waziri, *Advance Fee Fraud and Nigeria's National Security* (2007).

94 N. Jentzsch, op cit n 90.

telephone companies to activate their SIM cards.[95] With the exception of Liberia, Nigeria is perhaps the only African country with enforced biometric data capture as part of its personal information registration procedure.[96]

As privacy rights defenders such as Gow argues, the claimed effectiveness of compulsory registration in crime deterrence is doubtful. Lattice concurs with Gow that mandatory registration 'is ineffectual in those cases for which it is claimed it is most needed'.[97] There are others who claim it amounts to an unlawful invasion of privacy to collect the identity information of whole populations, who have not committed any offence, while going after a handful of criminals.[98] In view of the above, there has been a call for a balancing of privacy rights with the needs of public safety and security.[99]

The enactment of black letter of rules though is a commendable first step towards data security in Nigeria but it is still not enough as deterrence against abuse for several reasons. Imposing biometrics registration on whole populations is excessive and amounts to a knee-jerk response by the State to inadequacies of crime control that are unrelated to mobile phone usage. The NCC may not yet possess the technology to monitor surreptitious transfer of data by the more technologically advanced telephone companies and cyber hackers and criminals gives cause for concern. Also, unauthorised sales of subscriber information may be made by telephone companies to advertisers who could send unsolicited and nuisance mails to subscribers. It is also feared that network service providers may disclose location data of subscribers to law enforcement agencies without due pro-

95 Ibid.

96 K. P. Donovan and A. K. Martin, op cit n 25.

97 J Lettice 'Swiss move to block al-Qaeda mobile phone supply. The Register. Retrieved April 14, 2004, from http:// www.theregister.co.uk/2003/03/12/swiss_move_to_block_al/.

98 Office of the Privacy Commissioner of Canada. (2002). Privacy Commissioner's reply comments regarding the "Lawful Access" proposals. Retrieved January 15, 2016, from http://www.privcom.gc.ca/media/le_021125_e.asp; G. A. Gow and J. Parisi, Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones, (2008) 28 *Bulletin of Science, Technology & Society,* p. 61; N. Jentzsch, n. 90, p. 611.

99 G. A. Gow and J. Parisi, ibid.

cess.[100] The absence of a body independent of government in accordance with international best practices to mediate privacy rights between the NCC and telephone companies on one hand and subscribers, on the other, leaves a yawning implementation gap of the Regulations. While it may still be early to determine the overall effect of mandatory SIM card registration on privacy rights of mobile phone users in Nigeria, there is yet no data from law enforcement agencies as to percentage of crimes that are phone-related to justify the blanket measure. Furthermore, the veil of secrecy that traditionally surrounds law enforcement generally and national security in particular may ultimately becloud the future success of the Regulations.

Compulsory SIM card registration considering innovations in technological convergence is a threat to personal anonymity. The thinking that once data is secured in Central Data Bank to be housed at NCC headquarters is flawed. This is due to difficulties of regulating a technologically advanced industry like telecommunications where new technologies of data mining could easily render such data bases vulnerable to unauthorised access. National security agencies and the police could easily track a person's position and compile information on private conversations and relationships, banking details, e.tc. Even when possess lawful warrant to do so the necessary safeguards against misuse of information not connected to crime control activities, which may come into their possession has not been provided.[101] Considering the need for public safety and national security, the NCC Regulations has not addressed those narrow and exceptional circumstances when data may be retained or lawful interception of communications or transmission of information to third parties may only be carried out by judicial authorisation.[102] Predictability in regulating an industry underpinned by rapidly changing technology is critical for credibility of the regulator itself.

100 G. A. Gow, Information privacy and mobile phones, (2005) 11 *Convergence,* pp. 75-87.

101 The NCC is considering the adoption of formal guidelines on interception of communications for national security.

102 G. A. Gow and J. Parisi, op cit n 98.

4. Conclusion and recommendations

A rising digital economy such as Nigeria's calls for bold privacy protection. In the absence of meaningful legal safeguards, sectoral regulations such as the NCC Regulations may be welcomed, but are inadequate to protect and fulfil privacy expectations including data protection, dignity and other fundamental rights of subscribers. Despite the avowed goals of subscriber registration in Nigeria, the lack of a holistic legal framework to safeguard unlawful dealings in personal data of subscribers creates legal uncertainty as to subscribers' rights and liabilities vis-à-vis the State, the NCC, technologically advanced telephone companies and other data controllers in cases of unlawful data retention and illegal dealings. Considering the claimed ownership by the Federal Government of Nigeria to the Central Database of subscribers' biometrics and personal data there need for an intermediary body to step in and protect over 180 million Nigeria yearning for modern communication services. In the unlikely event of an immediate amendment to the Constitution to create a right to informational or data privacy, there is need for urgent enactment of a data protection law by relevant national authorities.

Tax privacy, Information Laws and Ethics

by Kanwal Deepinder Pal Singh[1]

1. Tax privacy, information laws and ethics

Privacy is threatened in diverse situations every day by everyone against people, society and the state. Indian privacy law is evolving in response to four types of privacy claims namely, against the press, against state surveillance, for decisional autonomy and in relation to personal information.[2] Privacy is an essential constituent of liberty, the deprivation of which prevents people from making fundamental choices. Right to privacy is not enumerated as a fundamental right in the Indian Constitution, but has been inferred so from Article 21 (Privacy as Decisional Autonomy).

The freedom of information aims to provide every citizen right to obtain access to government records. This increases accountability of the government and promotes fairness in administrative decision-making processes. The protection of privacy is based on the principle that information collected or one purpose should not be used for another purpose without the consent of the individual to whom the information pertains.[3] The right to information, being integral part of the right to freedom of speech, is subject to restrictions that can be imposed under Article 19(2).[4] Some authors argue that privacy is the expectation that information about a person will be treated appropriately. This theory of "contextual integrity" believes that people do not want to control their information or become inaccessible but they want their information to be treated in accordance with their expec-

1 Professor, University School of Law and legal studies, Guru Gobind Singh Indraprastha University, Delhi, India.

2 Acharya Bhairav, "Four Pillars of Privacy In India", Economic and Political Weekly", May 30, 2015, vol. 1 22, p. 35.

3 http://blog.onlinerti.com/2015/01/04/right-to-information-vis-a-vis-right-to-privacy/. Last accessed on 18 Nov. 2016.

4 http://cyfy.org/india-right-to-information-and-privacy-two-sides-of-the-same-coin/. Last accessed on 22 Nov. 2016.

tations[5] (Information Privacy).[6]

Information privacy is relatively recent in India. Personal information can cause the identification of a person, used directly or in conjunction with other information. Therefore information privacy law seeks to regulate the collection, use, storage, disclosure and destruction of personal information in order to protect the expectations of the individuals. State authorities collect personal information for the general purpose of governance, such as census, identification documents, licenses, passports, aadhar cards e.tc.. The right to receive information may lead to greater transparency in public life but it also might step upon right to privacy of certain people. There exists a certain conflict between the right to privacy and the right to information and the need to balance them has been part of academic debates. In India, this conflict or potential infringement has been balanced under Section 8 of the Right to Information Act, 2005 (the "RTI Act"). Section 8 provides that no information should be disclosed if it creates an unwarranted invasion of the privacy of any individual. The exception in S. 8(1)(j) prohibits the disclosure of personal information for two reasons:

i. its disclosure does not relate to any public activity or interest, or
ii. it would be an unwarranted invasion into privacy.

The above two conditions however get trumped if a larger public interest is satisfied by the disclosure of such information. The Bombay High Court[7] has decided that the exceptions to disclosure other than the right to privacy are not restricted by this provision. The interpretation given by the Court thus ensures that section 8(1)(j) still has some effect, in host of declarations and all sorts of information such as Income Tax Returns, e.tc. of both private and public individuals would have been liable to disclosure under the RTI Act.

The RTI Act defines the term information but does not define the term "personal information". The courts in India tried to draw a distinction between the term "private information" like, marriage, motherhood, procrea-

5 Ibid.

6 On contextual integrity and privacy see Helen Nissenbuum, "Privacy as Contextual Integrity", 79 Washington Law Review, 2004, pp. 119-158.

7 *Haresh Jagtiani v. State of Maharashtra* (2015).

tion, child rearing e.tc. and personal information" that pertains to an individual. Under the Act, all private information would be part of personal information but not the other way round. The term 'personal information' has been described as "identity particulars of public servants, i.e. details such as their dates of birth, personal identification numbers and as including tax returns, medical records e.tc.

The term "larger public interest" has also not been discussed or defined in the RTI Act. Courts have developed some tests to determine if in a given situation, personal information should be disclosed in the larger public interest. The term "public interest" denotes that the interest involved should serve a large section of the society and not just a small section of it.[8] The term "larger public interest" cannot be given a narrow meaning, was suggested in many decided cases on the right to privacy. Beginning with *Kharak Singh*[9] all the way to *Naz Foundation*[10] (Privacy and Surveillance) a wider connotation has been provided. In light of the Section 8(1)(j), two different tests have been proposed by the Courts, which lay the same principle in different words:

1. The test laid down in the case of *Union Public Service Commission v. R.K. Jain*[11] states:
   i. If the information sought does not qualify as personal information, the exemption would not apply;
   ii. Such personal information should relate to a third person, and
   iii. The information sought should not have a relation to any public activity involving third person, or in public interest.
2. The other test was laid down in the case of *Vijay Prakash v. Union*

8 *Union Public Service Commission v. R.K. Jain*, Delhi High Court W.P. (C) 1243/2011 & C.M. No. 2618/2011 (for stay), dated 13-07-2012.

9 AIR 1963 SC 129.

10 Delhi High Court, W.P. (C) No.7455/2001 dated 02-07-2009.

11 Delhi High Court W.P. (C) 1243/2011 & C.M. No. 2618/2011 (for stay), dated 13-07-2012. This ruling was overturned by a Division Bench of the High Court relying upon a subsequent Supreme Court ruling, however, it could be argued that the Division Bench did not per se disagree with the discussion and the principles laid down in this case, but only the way they were applied.

of India,[12] in the specific circumstances of disclosure of personal information relating to a public officials. This test states that situation where the personal information would not qualify for exemption. These situation can be enumerated as follows:

i. if the information is deemed to comprise the individual's private details, unrelated to his position in the organization;
ii. if the disclosure is with the aim of proper performance of the duties and tasks assigned to the public servant, and
iii. if disclosure will furnish information required to establish accountability or transparency in the use of public resources.

The constitutional right to privacy in India is also not an absolute right and various cases have carved out a number of exceptions to privacy in 'larger public interest'. Reasonable restrictions can be imposed on the right to privacy in the interests of the sovereignty and integrity of Indiamorality decency e.tc. The right to privacy can be restricted by procedure established by law. This procedure would have to satisfy the test laid down in the *Maneka Gandhi*[13] case.

Another decision in the *Rajagopal*[14]case lays down another test. It provides three exceptions to the rule that a person's private information cannot be published. They can be enumerated as follows:

i. person voluntarily raises or invites a controversy,
ii. if a publication is based on public records other than for sexual assault, kidnap and abduction,
iii. right to privacy for public officials with respect to their acts and conduct relevant to the discharge of their official duties shall not qualify for exemption.

Although the Court talks about public records, it does not use the term

12 2009 (82) AIC 583.

13 *Maneka Gandhi v. Union of India*, Supreme Court of India, WP No. 231 of 1977, dated 25-01-1978. The test laid down in this case is universally considered to be that the procedure established by law which restricts the fundamental right should be just, fair and reasonable.

14 *R. Rajagopal v. Union of India*, Supreme Court of India, dated 7-10-1994. These tests have been listed as one group since they are all applicable in the specific context of publication of private information.

'public domain' and thus it is possible that even if a document has been leaked in the public domain and is freely available, if it is not a matter of public record, the right to privacy can still apply. Discord occurs when privacy is claimed in lieu of a breach of confidence remedy as in Ratan Tata's ongoing petition in the Supreme Court in respect of the government's unauthorised disclosure of Niira Radia's intercepted communications and their subsequent publication (Privacy and Press Freedom)[15].

The most common problem arises regarding information of public officers. It is argued that income tax details, financial details, medical records, e.tc. of public officials should be disclosed. In case of some officers, it would serve the interests of transparency and cleaner government (hence serving a larger public interest). In fact, it has sometimes been argued that public servants must waive the right to privacy in favour of transparency. However this argument has been repeatedly rejected by the Courts.

Distinction has been made between information that is inherently personal or has connection with public functions. The Courts have concluded that there can be no blanket rule regarding what information can and cannot be disclosed when it comes to a public servant, and it would depend upon the circumstances of each case. The Supreme Court in *Girish Ramchandra Deshpande v. Central Information Commissioner*[16] has decided that personal information should not be disclosed unless a larger public interest is served by the disclosure. [17]

Presently, there is no specific legislation in India dealing with privacy. The protection of privacy and data can be derived from various laws pertaining to information technology, intellectual property, crimes and contractual relations. The right to privacy has further been encompassed in the field of torts which include the principles of nuisance, trespass, breach of confidence e.tc. Parties may agree to regulate use of personal information by means of a "privacy clause" or a "confidentiality clause". There are privacy obligations under specific relationships like doctor-patient, husband-wife, customer-insurance company or an attorney-client. The above princi-

15 *Ratan Tata v. Union of India* (2010).

16 2012 (119) AIC 105 (SC).

17 http://cis-india.org/internet-governance/blog/white-paper-on-rti-and-privacy-v-1.2. Last accessed on 28 Oct. 2016.

ple also receives legal recognition in ss. 123-126 of the Indian Evidence Act, 1871. Information Technology Act, 2000 (Section 65 and 66), Indian Penal Code (Section 403), The Indian Copyright Act (Section 63 B) Credit Information Companies Regulation Act, 2005 ("CICRA") are a few legislations protecting Privacy. The Privacy Bill, 2011 has been introduced to regulate the collection, use and dissemination of their personal information and provide for penalization for violation of such rights. Therefore, the right to privacy in India remains a *de facto* right.

2. Tax authorities and use/abuse of information

Privacy is a primary issue in developing countries. Privacy has to be examined in the context of tax evasion. Our focus shall be on the abuse of information by tax authorities. The challenges and scope of privacy rights extend beyond the use of information by the government agencies. Use of technology has provided access to information and has made it possible for anyone to obtain any information. Improvements in technology have also made it easier for tax administrators to observe transactions and taxpayers. There has been an increase in ability to trace transactions and has thus strengthen, the government's role as a tax collector. Taxpayers use technology to avoid tax, and it also leads to erosion of privacy.

Tax is a social responsibility of multinational corporations also specially in circumstances when government is reducing its expense which is having an impact on everyday lives of people. Many multinational companies, operating very successfully are not paying corporation tax by window dressing their profits. Companies seek to minimise their tax liability through "tax planning", using legal mechanisms like allowances, deductions, rebates, exemptions, and so on. Though tax planning is a tax compliant behaviour but there is a grey area between "tax planning" and "tax avoidance". Tax avoidance, is legitimate but aggressive using financial instruments not intended for tax eg, the use of overseas tax havens. Avoiding tax can be seen as operating within the letter, but perhaps not the spirit of the law. Unlike tax evasion, tax avoidance does not involve concealing information or lying. Instead, it involves structuring business transactions to ensure that less tax is payable than one might otherwise expect. Tax avoidance works through compliance with the precise letter of the law, not through breaking

the law.[18] Tax evasion involves knowingly mis-reporting the facts. There is no ethical justification for tax evasion. Ethics on the other hand has three facets:

- *Utilitarianism*, i.e. total happiness across the population aiming for maximum satisfaction of desires.
- *Deontology*, i.e. ethics based on the idea of duty.
- *Virtue ethics*, i.e. ethics which focus on the virtues we should have, and on what constitutes a virtuous life.

Taxation plus government spending are an obvious way to achieve redistribution of income to ensure that everybody gets something. Taxation and spending help to achieve wide resource distribution, but high rates of tax reduce investment and makes it hard to generate sufficient total resources. Unlike the utilitarian, the deontologist lays down absolute duties. One such common duty is to respect property rights of others . This could be interpreted to mean that there should be no tax at all, because tax is the forcible transfer of property away from taxpayers. On the other hand, the duty to respect property rights could be used to argue that any social resources one used should be paid for, even if one did not ask for those resources to be provided.

Virtue ethics can be a bit more helpful on the question of the justice of taxation. Several virtues seem more likely to be exercised if tax rates are moderate rather than being very high. There are also political arguments based on the fact that taxation is coercive. In *Anarchy, State, and Utopia* (1974), Robert Nozick argued that imposed taxation is a violation of our rights. He supported that property was mainly shared out among people initially by a process of acquisitions and then by exchanges. He argues that it is not the question that the existing wealth should distributed differently without a tax-levying state it might be possible that the wealth may not exist. These arguments though provide a different insight are not enough to legitimise high levels of taxation by the state.

18 https://philosophynow.org/issues/90/The_Ethics_of_Taxation. Last accessed on 17 Nov. 2016.

3. The objective of taxation

Tax can be used for all sorts of purposes like the distribution of incomes and wealth either by transferring cash from the rich to the poor, or by providing the same state services to everyone while taxing the rich more than the poor in order to pay for them. Greater equality may also be an accidental outcome of using the tax system for other functions of the state. It can also be a goal in itself. Taxation provides revenue for federal, state, and local governments to support services, infrastructure, and resources for the public good. The states also have a right to levy and collect taxes on goods and services sold within the state. Power of taxing the people and their property is essential to the very existence of government.

Some sacrifice of equity, it is often argued, is unavoidable in a situation where tax-payers stop at nothing to evade tax. Tax law is reconciled to living with leakage- but steps can be taken to make it difficult to evade tax and to raise the cost of evasion. Countries of the world are more adept in taxing incomes without deductions in some way or the other.[19] Tax culture is, thus, dominated by a mentality and practices of evasion and avoidance. This kind of mentality is constituted and legitimised through the social approval of non-compliant behaviour, knowledge of the politicisation of the tax bands and the demonisation of the taxes department. Unwillingness to pay on the part of taxpayers and unwillingness to collect on the part of tax officials are other reasons of accumulation of wealth. Tax avoidance is a universal feature of capitalism though avoiding tax does not necessarily result in an anti-tax culture. The state is caught in a contradiction. Not only is it the only body enforcing tax compliance but simultaneously it is also a body that creates formal institutions for tax avoidance and evasion. The compromised state has therefore not gained the necessary legitimacy or the capacity to implement its right to tax. This has profound distributional consequences. While corruption is the idiom in which the state is discussed, the much more fundamental problem is tax avoidance and evasion. Primitive accumulation and obligations to caste and kin are privileged over the public interest. As a direct result, those who do not pay tax struggle to gain access to public infrastructure

19 "Perverting the tax system, The Direct Tax Amendment bill", Economic and Political Weekly, vol. 23, no. 3, Jan. 16, 1988, p. 71.

and services. No culture, however, is unamenable to change. Tax relationships are not only the products of rules and voluntary compliance, they are regulated through coercion mediated by relationships of class, caste and faction, which are structures of accumulation mostly not regulated by the state[20].

Information reporting and withholding is an important task of tax administration. They bring together information from different sources and verify it. Tax laws in most countries already require various private and public agencies to furnish information. In some cases agencies are also supposed to withhold a part of the payment made by the agent to the potential taxpayer. An efficient system of monitoring is required to collate and store data with easy access for retrieval and cross-checking. From an administrative perspective, most taxes collected in developing countries come from a relatively small number of population. Accurate tracking of fiscal flows is critical to successful tax administration. Before devoting much effort to this difficult task, however, it is critical to ensure that tight control is maintained over the payments and liabilities of large taxpayers. Tax agencies used Information Technology T mostly to process tax returns and payments. Returns contain taxpayer identifying information, details on gross income received from various sources, e.tc. In many developing countries like India, large section of population does not file returns at all, because their income tax obligations are considered to be fully satisfied by the tax withheld by their employers. Even in developed countries like the United Kingdom most personal income taxpayers do not have to file returns because cumulative averaging results in the correct amount being withheld. Countries, such as Australia, are also considering "return free" systems that relieve most taxpayers from the obligation of filing a return. Such systems have obvious attractions for both taxpayers and the tax administration.

Adopting new technology carries with it potential pitfalls as well as potential gains. Conceptions of rights to privacy differ among societies. There have been developments which say that most of the information that tax authorities need is needed is already contained in the central computer and should be correspondingly processed. This vision is already a reality in Singapore, where withholding has been taken to its logical limit so that the

20 Amrita Jairaj and Barbara Harris White, "Social Structure, Tax Culture and the State", Economic and Political Weekly, Dec. 13, 2006, p. 5252.

government can transfer funds directly from a person's bank account to the treasury to settle tax liabilities as calculated by the government. Therefore the real danger from new technology may not be the erosion of the tax base as taxpayers use technology to avoid tax, but the erosion of privacy as governments take defensive action. It is therefore a requirement that citizens should reach a consensus that permits access to private activities necessary for the sustenance of their public communities, without allowing such information to be misused. This may also be called "the transparent society" - one in which people are held accountable for their actions, including what they do with the information to which they have access. Countries around the world, developed or developing, need to balance the benefits of providing taxing authorities with additional tools and resources, against the costs of invasion of privacy and potential for abuse by government officials.[21]

To date, most privacy legislations in developed countries have focused on protecting the rights of individuals. EU Data Protection Directive provides rules for private-sector processing of personal information. The US Privacy Act of 1974 sets forth guidance for the use individual data by the federal government. There should be designs and methods in order to ensure institutional accountability. Legal and political institutions provide sufficient checks and balances to allow use of the information generated by improvements in technology without the likelihood of substantial abuses. Given the diversity of cultures and societal norms, there exists a wide range of tolerance and intolerance for measures that infringe on privacy. Many policy initiatives adopted by governments may challenge personal privacy. Such initiatives include many of the technologies that may be used to improve the tax system like the use of identity cards using fingerprint and iris scanning biometrics e.tc.

Countries with good tax administrations also score well in privacy rankings. On the whole, however, it seems probable that, if tax administrators were to improve significantly their capacity to acquire information, countries also need to have adequate procedural safeguards to offer sufficient

21 Richard M. Bird and Eric M. Zolt, "Technology and Taxation in Developing Countries: From Hand to Mouse", National Tax Journal, vol. 61, no. 4, Part 2: Technology, Privacy, and the Future of Taxation (December, 2008), pp. 791-821, National Tax Association Stable, http://www.jstor.org/.

privacy protection. The costs of disclosure of information may also differ among developing countries. In Colombia, for example, one reason offered by some for the recent discontinuation of the long-standing wealth tax, in existence since 1935, was the fear that the misuse of this tax information might increase the risk of kidnapping. In current environments when tax information is misused, the barriers against such misuse should clearly be very high. If it is not possible to erect and enforce adequately such barriers, then it may make sense not to collect the information, even if it prevents tax administrators from making distinctions among persons and the tax base that would theoretically improve the tax system.

4. Conclusion

The last few years has seen a spate of rights-related legislations related to information, employment, and education. But this package of laws is incomplete without a fundamental right to participate in decisions relating to development, welfare, and conservation.

Every citizen needs to have the right to be consulted, and his/her opinion and judicious use of information to be part of the considerations for decisions in governance. This shall enable citizens to participate meaningfully, through proactive provision of information (taking forward the suo motu provisions of the Right to Information (RTI) Act. Links would need to be made between such legislation and the relevant existing policies and laws, such as the RTI Act, the panchayat laws, and others. Checks and balances would need to be built in to ensure against misuse and against indefinite stalling of decisions. This can help the abuse of power by international corporations, and the financial elite, and help the majority of Indians who desperately need meaningful development. This would tackle the various forms of corruption specially taxation problems in India.

Rather than hiding behind the business case for tax avoidance, businesses need to be transparent about their tax planning. Both companies and government need to pay more attention to communicating their position on this issue and their interpretation of the law – and above all they need to be open about it. This would restore public trust and bring more

certainty for business.[22] Today there are no compartments in the world. Capitalist pursuits and societal imperatives need to be balanced. Indeed, through tax avoidance the corporation contributes significantly to an overall decline in government services, which ultimately degrades the operating environment and the very markets within which the corporation seeks to thrive. The future of society is dependent on the capacity of the state to balance ethics privacy and transparency. An interface between them directly affects the dignity of the population. Multinational corporations shielding profits from meaningful taxation have troubled governments and individual taxpayers alike. Corporate taxation is a worthy public goal that companies should do voluntarily. There should be an ethical framework within which corporate officers, boards of directors, shareholders, tax advisers, and stakeholders should operate. The higher ethical perspective demands that corporations rise above minimal compliance standards on taxation and work towards a transparent society. The Corporations should not blind eye to the larger issues affecting the livelihoods and dignity of ordinary people. International tax authorities are working towards create a common template for multinationals to report to tax authorities. It will help the developing countries to collect the taxes owed them, with access to the global tax information they need[23].

22 http://www.theguardian.com/sustainable-business/avoiding-tax-legal-but-ever-ethical. Last accessed on 22 Nov. 2016.

23 Organisation of Economic Co-operation and Development (OECD), reflecting concerns among the major economic powers, has become particularly focused on the problem of tax avoidance, especially the issues of base erosion and profit shifting (the basic tools of tax avoidance), as prominently demonstrated in a February 2013 report, which was followed a few months later by a statement of recommendations. At their June 2013 summit in Northern Ireland, the leaders of the G20 affirmed their support for the OECD's work in this area publish national Action Plans to make information on who really owns and profits from companies and trusts available to tax collection and law enforcement agencies." In mid-July 2013 the finance chiefs of the Group of Twenty nations fully endorsed "the ambitious and comprehensive" plan set forth in the OECD's report on corporate tax avoidance, Action Plan on Base Erosion and Profit Sharing, and recommended that G-20 leaders approve the Action Plan during their September 6 2013 summit. On September 6,2013 the G20 leaders, meeting in Saint Petersburg, Russia, followed with full endorsement of "the ambitious and comprehensive Action Plan—origi-

Countries need to balance the benefits of providing taxing authorities with costs of invasion of privacy and potential for abuse by government. However, the availability of different types of information may also result in government officials using information for financial gain, political gain or discrimination, or simply for the thrill of invading the privacy of well-known individuals. Government officials could also use information not for personal gain, but in a manner in consistent with the laws governing privacy in order to achieve what they believe is good government policy.

State leaders believe that a technology solution can be found to make the tax system more balanced and fair. Tax policies should be underpinned by the guiding ethical principles of accountability, transparency and consistency. Tax planning arrangements that go beyond the intent of the law are not ethical. Apart from companies, government and business should ensure that corporate tax contributions are a demonstrably fair return to society. Citizens on the other hand should permit access to private activities for the sustenance of public communities, without allowing such information to be misused. People should be accountable for what they do with the information to which they have access.

nated in the OECD.

INTELLECTUAL PROPERTY

a. theory

Sharing is Caring vs. Stealing is Wrong: A Moral Argument for Limiting Copyright Protection

by Julian Hauser[1]

1. Introduction

Interest in copyright has ebbed and flowed ever since its inception more than two hundred years ago. The debates brought on by the tidal wave of digitisation are however of a rare intensity. Copyright holders sue their own customers in the thousands (Kravets, 2008). Authors decry the public's unwillingness to respect their «right to the protection of the moral and material interests resulting from [their work]» as set down in article 27 of the *Universal Declaration of Human Rights*. Others–consumers as well as authors–decry the culture industry's monopoly on human creativity; a worry about which the famous Twitter persona Nein succinctly tweeted: "Another beautiful day for the Culture Industry. For culture, not so much." (Nein, 2013). Users of unlicensed copyrighted material are labelled pirates, a word that carries connotations of robbery, violence, and anarchy. In retaliation, the term been re-appropriated and users have gone on to found political parties that advance their views: the pirate parties. These parties see themselves as part of wider culture of collaborative creation and creative re-use, which finds copyright protection to be hindering their efforts of attaining a more cooperative, democratic, and "bottom-up" mode of production (Aigrain, 2012). Copyright, in short, is at the forefront of public discourse.

What was "once taken for granted as morally legitimate" (Himma, 2008, 1143) is now up for discussion. While balancing authorial with public in-

1 University of Edinburgh, School of Philosophy, Psychology and Language Sciences – University of Berne, Philosophy, Graduate Student, email: julian@julianhauser.com

terests is as essential today as it has been for centuries, computerisation and the internet present us with radically new ways of resolving this tension. The renewed debate on copyright has led to a decline in relative importance of the more technical matters of copyright law, benefiting fundamental discussions of the permissibility of copyright protection and the form and scope of a moral regulation of authorial works.

The literature on the ethics of copyright largely adheres to a distinction between three different approaches: a utilitarian approach (sometimes replaced by a value pluralist consequentialism), accounts based on the Lockean theory of labour desert, and lastly personality interest theories fashioned after Hegel (and sometimes Kant)[2]. A combination of two factors renders this separation problematic. Firstly, the approaches are presented as clearly distinct and stemming from fundamentally different streams of thought. While there is ample criticism of each individual approach, there is little research on the interactions between the different approaches. Secondly, only few philosophers argue that a single approach is sufficient to morally justify copyright (Resnik, 2003). Most proponents of copyright think a combination of the three arguments can compensate for their individual weaknesses. However, while an approach focusing on the different accounts individually might be suited to show what speaks for each approach *per se*, it does not lend itself to the establishment of a general account of the morality of copyright.

In this paper I try to sketch a big picture account of the morality of copyright, analysing the key strengths and weaknesses of the various approaches. I hope to show that the case for copyright is far weaker than often assumed and that a weighing of the different interests is more likely to come out in favour of a substantially reduced set of rights for authors. I propose a set of rights that I believe is in accordance with the moral interests at stake.

In the next section I will set down the basic principles of copyright law, in section three I analyse public interests, in section four Lockean approaches, and in section five personality interest accounts. Section six investigates what rights these interests give rise to, section seven looks at contributors, and the last section concludes.

2 For examples of this separation see Moore (2008) or Hughes (1988).

2. Copyright law

Arguments for and against copyright suffer from a notorious problem – there is no single thing called copyright. In fact, there exists not only a myriad of currently existing legal systems but also a spade of previously prevalent systems and of course an abundance of theoretically possible systems. And they all have a claim to the term copyright. In the following I define a *minimal copyright system*: a system exhibiting a number of principles that are defined in international law or present in (almost) all jurisdictions.[3]

The purpose of this exercise is to force the moving target that copyright is to hold still. A successful attack on the minimal copyright system does not necessarily imply that all copyright systems are morally unjustified – additional principles could still improve copyright's lot. However, by showing that copyright is morally problematic at its core, I hope to show that it is unlikely to be rescued by additional adhoc principles. Defining the basic principles should also help us pinpoint exactly where copyright goes wrong and what features a non-copyright regulation of authorial works might have. I want to stress that I have no interest in semantic squabbles – if you think the principles I define towards the end of this paper constitute copyright, then so be it.

In order to define the minimal copyright system two aspects need to be explored: (a) the subject matter of copyright and (b) the rights granted by copyright. The subject matter defines to which works copyright applies, whereas the rights granted define the bundle of rights accorded to the author of such works.

The scope of the subject matter of copyright is very wide. The *Berne Convention* defines as copyrightable every type of "production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression" (cited in Dutfield, 2008, 78). Most countries rely on the concept of *originality* to determine whether a certain work is protected by copyright

3 The most important and widely ratified international treaties on copyright are the *Berne Convention for the Protection of Literary and Artistic* (Berne Convention) from 1886 (last revision in 1971), the *International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations* (Rome Convention) from 1961, and the *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS) from 1994.

(Abbott, et al,. 2011). Originality is a concept "fiendishly difficult to define" (Dutfield, 2008, 79) but this need not concern us; at this point it is enough to understand that in today's copyright law, originality requires that a work of authorship exhibit a minimal level of creativity[4].

Minimal degree of creativity: copyrightable works need to exhibit a minimal degree of creativity.

The notion of *expression* is also essential to any conception of copyright. Only expressions are copyrightable, thereby excluding ideas, methods, functions and facts from being the subject of copyright (Abbott, et al., 2011). This can be illustrated by the fact that only the text of a book can be copyrighted but not the ideas expressed therein.

Idea/expression dichotomy: only expressions are copyrightable.

When it comes to the rights accorded by copyright, the matter is complicated by the fact that there are *economic rights* as well as *moral rights*. In most jurisdictions moral rights are considered a separate body of rights or might not exist at all.

Economic rights can be transferred and are thus tradeable on the market. Historically, the right to make copies was the first such right. To this right many more have been added since, for example the right to modify a work, the right to communicate a work to the public, and more. I focus on the three rights I have just explicitly mentioned as they are the most basic. However, I believe my argument applies to all existing economic rights, and as such a different selection of minimal economic rights should not affect my assertions.

Minimal economic rights: copyright protects for a limited amount of time one or more of the following transferable rights: the right to make and distribute copies, the right to communicate a work to the public, and the right to make modifications.

4 My notion of creativity should be seen as very thin and encompassing the US American legal notion of *creativity*, British copyrightability notions of *skill* and *judgment* as well as the continental European concepts of *creative choice*, *intellectual contribution* and again *creativity*.

Only economic rights are part of my definition of the minimal copyright system as moral rights only exist in some jurisdictions and always in addition to economic rights. Moral rights cannot usually be transferred and may hold in perpetuity. My criticism of copyright applies to most moral rights, too. While I retain the right of attribution – the right to be named as the author of one's works – I do argue against the second important moral right: the right of integrity. This right allows authors to object to modifications of their works that endanger their reputation.

Both economic and moral rights are held by the author alone; she can exclude anyone from using or appropriating her works. Non-authors do not enjoy any of the copyrights, except if these are transferred to them by the author.

Exclusivity: economic and moral rights must be exclusive to the author.

3. Public interest arguments

Our lives are inextricably intertwined with copyrighted works, used daily by probably a majority of the human population. We listen to music, read books, use word processors to write academic papers, consult written manuals, and go to the cinema. I believe it is reasonable to assume that the use of copyrighted works increases our welfare–why would people go to such lengths and incur such costs to acquire them otherwise? According to the public interest view, it is this increase in welfare that justifies copyright. It is not because of authors but because of the general public that we need to protect authors.

The argument can be summarised as follows: Copyright allows authors to use the power of the law to exclude people from using their works. This enables authors to gain financially from the sale of their copyright or of copies of their works. Because of these financial incentives authors produce a higher volume or higher quality of works, and the public benefits from these works because authors will–for a fee–grant access to them. The negative effects of the fee barring some people from accessing the works they desire is counterbalanced by the positive effect on those users who have access to works that would not have come into existence without copyright.[5]

5 Furthermore, to minimise the negative effects on those who are not able to use copy-

I now turn to the plausibility of the premises necessary for the validity of the above argument. I have organised these into three groups. The first group is the most obvious and is considered by most welfare-based accounts and by my argument sketched above. The second is a necessary but often forgotten addition to the welfarist approach and the third goes beyond welfare and considers additional public interests.

The need for the first three premises should be clear from my description of the welfarist argument.

(C1) Copyright enables authors to benefit financially from their works.

(C2) Potential financial benefit acts as an incentive to authors to produce a higher quantity or quality of authorial works.

(C3) The consumer and producer benefits caused by copyright outweigh the consumer and producer harm.

Does copyright enable financial profit for authors as stated in (C1)? Copyright restores excludability and thus enables authors to ask for and receive monetary compensation for access to their works. In many economic sectors there is little doubt that copyright does benefit authors tremendously. However, in other sectors there exist powerful middle men who can siphon off the profits. For instance, only twelve percent of musicians' income in the United States derives directly from copyright with the highest earners taking home most of the share (DiCola, 2013). Where authors do not currently profit from copyright, it can be argued that this not because of copyright *per se*. If the market mechanisms were to be relevantly regulated, it might be possible to correct the current power differentials between authors and content providers. In conclusion, copyright does enable at least some authors to benefit financially from their works. However, the real benefit must be critically assessed, taking into consideration that many authors do not benefit financially – or only benefit marginally – from copyright.

I believe two things are clear when it comes to premise (C2). Firstly, authorial works are not created for pecuniary gain alone. Many authors do

righted works, most regulatory systems provide for exceptions to the rights they grant. Sometimes called *fair use* or *limitations and exceptions*, these aim to ensure that the public does not suffer unduly high costs and that authors do not misuse their powers (Dutfield 2008).

not profit from copyright but produce works regardless. Secondly, financial gain has an incentivising effect on many producers (Ryan and Deci 2000; Douglas et al. 1998). The precise role monetary and non-monetary incentives play in the production of a specific work depends both on the author as well as the work's characteristics. However, it is clear that financial benefits do act as incentives for at least some authors. And because it is *potential* financial benefits that incentivise authors, copyright can be effective also when only few authors profit in practice. I therefore sustain premise (C2).

Premise (C3) is where the economic calculus becomes complex indeed. A first step in appraising (C3) consists in adding the consumer and producer surplus achieved by a higher quantity and quality of authorial works. The uncertainties regarding (C1) and (C2) have already shown some of this task's difficulties. Additionally, we need to factor in the costs caused by higher prices – these entail that people who would have benefited from access to authorial works that would have been produced even without copyright and who do not have the financial means to pay for them are left with less welfare with copyright than without. Furthermore, costs of legislation and enforcement need to be considered. There is also evidence that some forms of monetary incentives crowd out non-monetary incentives, which if true for authorial works, means the positive effects of copyright on the monetary incentives postulated in premise (C2) are counteracted by negative effects on other forms of incentives (Moore, 2008). Additionally, producers themselves can be harmed by copyright when they desire to base their works on prior and copyrighted works. The empirical debate about this calculus has raged for a very long time, and there has so far been no comprehensive victory for either side (Abbott et al. 2011). We are thus left in empirical limbo with regard to this premise.

The challenges faced by the public interest theorist are formidable when considering premises (C1), (C2), and (C3). And, to make matters worse, the proponent of copyright needs to supplement these premises with:

(C4) The welfare calculus of alternative compensation systems is worse than copyright's.

Premise (C4) is necessary because copyright is not the only means by which the production of authorial works can be financially incentivised. This premise often remains hidden and its truth assumed when the usefulness of copyright is, for instance, demonstrated with copyright's contri-

bution to GDP. Possible implementations of alternative compensation systems are currently hotly debated in the field of economics (Liebowitz and Watt, 2006). These schemes can be divided into two groups: compulsory government-mandated contribution schemes and voluntary contribution schemes. Both have their advantages and disadvantages, and a non-copyright system might also use a combination of some of these schemes to provide effective monetary incentives. What is more, an alternative system need not necessarily be as effective at providing monetary incentives as the copyright system. If the costs associated with such an alternative system are lower than in the copyright system, then this has to be factored in, too. What is more, already today not all monetary incentives to authors are due to copyright. It must also be noted that the less clear premises (C1), (C2), and (C3) work in copyright's favour, the more difficult it becomes to argue that (C4) is true.

There is clearly no consensus among economists on whether copyright is the best way to boost the production of authorial works. However, if anything, there is a tendency of doubt about copyright's usefulness. Moore – referring to the work of Machlup, Priest, and Long – writes: "Economists who have considered the question indicate that either the jury is out, or that other arrangements [than copyright] would be better" (Moore 2011). Even if I cannot conclusively reject the truth of premise (C4), it is clear that the proponent of copyright has a lot of work to do to turn it into an argument that can lend strength to her point of view.

Finally, the welfare economic argument needs to fend off two additional attacks. Firstly, market relations might not be the only relevant way in which one can analyse welfare. Secondly, there might be values other than welfare that are important in assessing what policies are good for individuals and society. The first argument is about how to measure welfare and says that, for instance, power relations and non-market factors need to be considered, too. The second argument proposes a value-pluralist account.

(C5) The overall effect on the attainment of moral values is better in the copyright system than in all other regulatory system.

Under the above premise it remains possible to claim that we should only strive for economic welfare, but now an argument for such a claim must be supplied. I will content myself with supplying some hints about why such an argument is difficult, and why value-pluralism makes the argu-

ment for copyright even more onerous. For example, utilitarianism does not consider the importance of the diversity of works for people's ability of self-expression and personal development. There are indications that the top-down distribution symptomatic of a culture industry based on copyright reduces diversity (Aigrain, 2012). Another point is made by Gillespie, who writes that "[c]opyright is at the heart of cultural policy – those rules that help to govern what is said, by whom, and with what effect" (Gillespie, 2007). With copyright, authors, copyright holders, and the financially well-off have a favoured access to works and are thus in a privileged position when it comes to deciding on the future development of our culture and associated values. Distributive justice is also clearly affected by copyright, as those without the necessary means cannot access copyrighted works. This not only lowers their welfare but also bars them from acquiring information necessary to improving their situation (Murphy, 2012).

To conclude, I believe (value-pluralist) consequentialism draws our attention to important concerns about copyright. I hope to have shown that it is very difficult to make a conclusive argument for copyright using such an approach, and there are strong indicators that consequentialism favours alternatives to the copyright system.

4. Lockean aproaches

I will now turn my attention to those who lend their name to the French *droit d' auteur* and the German *Urheberrecht*: authors.[6] How can their interests form a basis for the justification of copyright?

A successful account based on authorial interests is clearly insufficient for a conclusive judgement about the morality of copyright. Either authorial interests need to be balanced against the interests of the public or the account needs to be complemented by an argument dismissing the importance of public interests. However, it is clear that a successful authorial interest argument for copyright weighs heavily in favour of copyright regulations. Himma even thinks any justification of copyright «clearly depends on whether authors have a moral right in the content of their creations» (2008, 1152).

6 These terms translate as *author's rights*.

Authorial interest theories come in a variety of guises. One prominent strand of thought is formed by those approaches that are based on Locke, and this is the focus of the present section. I hope to show that Locke's original theory is fatally flawed when it comes to justifying copyright and that this flaw is inherited by later Lockean theories. John Locke's *labour desert theory* of material property can be divided into four main parts, which I will shortly sketch here.

According to Locke (1764, bk. II, ch. V), God gave the earth to man in common, to be used to their advantage and convenience.

(L1) Resources exist to be used by people.

For a person to enjoy the earth and what it produces, she must be able to exclude others from use of the good she desires. And in order to exclude others legitimately, a person must be the owner of that resource.

(L2) Enjoyment of a resource requires the ability to exclude others from using it; legitimate use requires ownership.

The fundamental question for Locke concerns how initial appropriation can come about. Locke's starting point is that human beings have ownership in themselves. This ownership extends not only to the body but also to the activities undertaken with it, *inter alia* labour. When working the land, people mix themselves, in the form of their labour, with the land. By mixing one's labour with the land, the land becomes an extension of the person and thereby the labourer's property.

(L3) People come to own a resource by mixing their labour with it.

The extent of the acquisition of property is however limited by two conditions. (L1) and (L2) postulate that resources are appropriated to be enjoyed – consequently appropriation that goes beyond what can be enjoyed is illegitimate. In this spirit, the first limitation states one may only acquire as much as one can use for oneself – if appropriation leads to waste it is not legitimate. Secondly, one may only acquire so much that there is enough and as good left for others after appropriation.

(L4) One may only acquire as much as one can use for oneself and only as long as there is enough and as good left for others.

Much criticism of Locke focuses on (L3) as it is not at all clear why mixing one's labour with a resource should lead to an extension of ownership rath-

er than a loss. Nozick (1974) came up with the famous example of someone who throws a can of tomato juice into the ocean, asking whether this should really be enough to acquire ownership of the sea.

Contemporary authors try to remedy this weakness by replacing the idea of the mixing of labour with other factors deemed morally relevant. Fisher (2007) argues that the expenditure of personal resources or effort gives rise to moral interests in the things that are thereby created. Himma (2008) proposes to see time as the crucial resource that is being used in authorial creation. Spinello (2003) argues that it is added value that matters. Nozick (1974) himself suppresses (L3) entirely and simply states that appropriation is legitimate up to the level proscribed by (L4).

All these approaches focus on (L3) or (L4) while crucially leaving (L2) unchanged. But in the case of intellectual resources, it is simply not true that we need to exclude others in order to enjoy a resource. Copyright protects abstract types, not material tokens. If I write a book, I do not necessarily become the proprietor of the physical book I write – I might have stolen the paper – but rather am accorded copyright of the text contained therein, that is to say, in the meaningful combination of the symbols that comprise the text.[7] This means what is protected by copyright is non-rival. The same abstract authorial work can be used by an infinite amount of people, without anyone's enjoyment thereby being degraded. In the case of authorial works use does not require excluding others. Therefore appropriation is not necessary for legitimate use, and (L2) cannot be employed to justify the necessity to appropriate authorial works.

The argument so far is not new. Lockean theorists claim to be able to evade the above challenge c. In fact, what is protected by copyright is not even the meaningful combination of symbols but some meaning of this combination of symbols. This explains why a translation of a work is also covered by copyright – even though the meaningful symbols are entirely

7 In fact, what is protected by copyright is not even the meaningful combination of symbols but *some meaning* of this combination of symbols. This explains why a translation of a work is also covered by copyright – even though the meaningful symbols are entirely different, the meaning of the symbols remains. The fact that meaning and expression cannot be easily differentiated is at the root of the difficulties regarding the idea/expression dichotomy.

different, the meaning of the symbols remains. The fact that meaning and expression cannot be easily differentiated is at the root of the difficulties regarding the idea/expression dichotomy.

Concerning (L2) by letting (L3) do all the argumentative work. I agree that a variant of (L3) can possibly be used to argue why certain people come to have certain rights to a given resource or authorial work. Maybe creating something valuable does create rights. The crux of the matter however is that not only authors create value with regard to authorial works. In fact none of the proposals for (L3) is limited to authors. Someone can interpret an authorial work and add value, someone can laboriously copy it, or spend huge amounts of time carefully reading it. Without (L2) justifying why authors need to be able to exclude others from using their works, all these people should be accorded rights, too.

There are two steps to the problem. Firstly, the inapplicability of (L2) leads to the loss of an argument for one essential aspect of the notion of property: exclusivity. Secondly, all proposed replacements of (L3) fail at restricting rights to only those who create a work, namely those that we commonly consider to be authors. And this is why all Lockean theories fail.[8]

An objection to my argument is expressed by Spinello and Bottis (2009). Their Lockean approach emphasises the idea that violating copyright harms owners. They base this argument on Locke's no harm principle (Locke 1764, bk. II, ch. II). But what is the harm involved when a person uses another's work without their authorisation? Clearly, the harm in question cannot come from inability to enjoy the work – no such harm exists with non-rival authorial works. Could it be harm to the ability to monetise the work? As I have shown in the section on public interest accounts, copyright is neither very good at ensuring this ability nor does it provide the only way of monetising authorial works. Furthermore, we do not always protect people's ability to make money, and we would therefore need an argument why such protection is warranted in the case of authors. Nonetheless, I think the notion of harm is relevant to our case. I will explore this idea in the next sections but as you will see this means leaving Lockean theories behind.

The failure of Lockean theories holds a promise. If we find a morally

8 Locke applied his theory only to material goods and can therefore not be blamed for the failure of Lockean theories on copyright.

valuable feature unique to authorship, we can let (L3) hold the whole argumentative weight without needing to be supported by (L2). This will furthermore enable us to see what harm authors may expose themselves to when publishing their works.

5. Personality interest

Personality interest theorists think they know what feature of the creation of works gives rise to authorial interests, and they think this feature can take on all the argumentative weight. In this section I introduce the personality interest account, sketch how authors come to acquire such an interest, and argue why it merits being protected.

The personality argument under its many guises takes inspiration from Hegel (for example: Hughes 1998) and sometimes Kant (for example: Lucibella, 2010). What unites these approaches is the «idea that an individual enjoys an exclusive moral claim to the acts and content of his or her personality, personality being understood to include a variety of character traits, dispositions, preferences, experiences, and knowledge» (Himma, 2008, 1155). Many authors stress the importance of external objects in people's quests for self-actualisation and for the development of their own personalities (Resnik, 2003; Hughes, 1998; Himma, 2008; Rawls, 2000). In order to become who we want to be, to develop life plans and follow them through, we need to control external resources. Authorial works are crucial for personal self-actualisation and therefore merit being protected.

Personality interests are diverse and not exclusively authorial. Many people see for example their wedding rings as integral to their personalities. Therefore an authorial personality interest account needs to show what interests are specific to authors and why these trump other people's interests in authorial works.

What personality interests could be exclusive to authors? Hughes (1998) has three proposals: sourcehood interests, intentionality interests, and creativity interests. I will not discuss the first two[9] as their scope is larger than

9 Sourcehood interest denotes the interests we may have in objects when we have been implicated in the causal chain of events that has brought them into existence. Intentionality interests are interests in objects that we have intentionally brought into exist-

what is protected by copyright. The third is however promising; creativity is an important aspect of the definition of the legal subject matter of copyright, and – as we will see – it is closely connected to our personality. In order to illustrate how creativity can underpin the moral justification of copyright, I will first explain what I mean by creativity, then shed some light on the connections between creativity, personal input, and personality interest.

The seminal case *Feist Publications, Inc. v. Rural Telephone Service Co.*[10], decided by the US Supreme Court in 1991, illustrates the legal notion of creativity. The matter of contention was an alphabetical list of telephone numbers compiled by Rural, the entries of which were copied by Feist and published in their own telephone directory. Rural consequently sued Feist alleging copyright infringement, prompting Feist to challenge the copyrightability of the work in question. This question of copyrightability–and not the matter of copyright infringement–forms the core of the case. The US Supreme Court decided in Feist's favour, arguing that a simple alphabetical ordering of telephone numbers, as in Rural's directory, does not display any creativity and is therefore not copyrightable.

While *Feist v. Rural* is intuitively comprehensible, it is very difficult to put one's finger on what exactly makes something creative. I will rather inelegantly evade this problem and adopt Hughes (lack of an) explanation. Hughes (1998) states that in some cases we cannot ascribe an object's coming into existence to external factors, which we perceive as mechanistic or random. In these cases a person is responsible for creating said object because this person's personal input explains why the object has come into existence. In the following, I will simply assume that personal input exists and that a certain degree of it is necessary to call an activity and the product thereof creative. Let us furthermore assume that creativity adequately tracks who is to count as an author, that is to say, that an appropriate level of personal input defines creativity, which in turn defines what is an original work and who is an author.

So far I have linked authorship to creativity and creativity to personal input. However, the connection between personal input and personality

ence.

10 499 U.S. 340 (1991).

interest still needs to be explicated. Authors are divided on whether personal input necessarily implies involvement of the author's personality. Some authors, such as Dewey (1980), claim that all creative endeavours are marked by our interests, whereas others, such as Hughes (1998) argue that some authors create original works without these being connected to their personality. We need not resolve this matter; even the latter approach does not endanger a personality interest argument for copyright. A proponent of copyright can argue that those cases in which authors do form personality interests are of such importance that they merit offering copyright protection to all those who might potentially benefit from it. Summarising the argument thus far, personal input is what makes works creative and this personal input – at least regularly–leads to the author's personality being extended to, or expressed in, the works they create[11].

Hughes identifies two potential objections to the authorial personality interest account: «[i]t may be wrong for people to (1) identify with their capacities; and then, (2) identify with the intellectual products of those capacities» (Hughes 1998, 84). I do not believe it can be wrong for people to identify with their capacities. Individual personal capacities are an essential part of who we are. What is more, also our moral and political convictions and our intimate fears and hopes can be expressed in what we create. To demand that people not identify with these elements of their personalities is tantamount to asking them not to identify with themselves. This is both impossible and morally wrong.

But why should these personality interests extend to authors' creative works? Hughes argues that this is the case because our productive life–the sense of imprinting ourselves on the outside world–is essential for our self-actualisation (Hughes, 1998). And because an author's ability to develop herself can be harmed when other people use or modify her works, authors deserve to see their interests protected.

11 The idea of an extension of personality also shows that personality interest approaches should not be seen as entirely unrelated to Lockean approaches. In fact, it is possible to interpret Locke in a way that renders his theory to a large extent compatible with a personality interest theory. Hughes–quoting Rapaczynski–writes that: "[s]ome writers have suggested that Locke actually subscribed to such a personality theory in which 'applying one's labor to a natural object ... endow[s] it with certain features pertaining to one's own form of existence'" (1998, 28).

6. Regulating authorial works

Consequentialism and personality interest accounts shed light on the moral interests authors and the public may have in authorial works. In the remainder of the paper, I want to explore a minimal set of principles that protect these morally valuable interests and argue why these are sufficient.

Attribution: authors have the right to be attributed as the authors of their works if doing so is possible with reasonable expenditure of resources.

Attribution ensures that people are recognised for being authors, which can in itself be a valuable recognition of people's agency (Hughes, 1998). Moreover, without attribution it is difficult for authors to gain reputation, which functions as an important form of social recognition. Human beings are social animals, and without social recognition most people will fail in their quests for self-actualisation. Social recognition is also connected to access to material and social resources that are essential to further self-actualisation.

Attribution does not generally hinder the public's ability to freely use, modify, and distribute authorial works. The right of attribution also incentivises authors to produce works and in that sense advances the public interest. Moreover, society would be hard-pressed to support and recognise important contributions without knowing who contributed what. However, the public interest in identifying authors does not justify an obligation to attribute authorial works. Being able to publish works anonymously can be tremendously important, be it for personal, political, or artistic reasons. Should authors be able to waive the right of attribution? If authors are not obliged to use their right of attribution, then I would follow a liberal argument and claim they should be able to permanently waive that right as well.

The public must try to attribute works correctly, which may involve developing schemes that facilitate locating authors and attributing works correctly. However, if, after expenditure of a reasonable amount of resources, it still proves impossible to correctly attribute a work, then the public interest trumps the authorial interest and the work may be used without attribution[12].

12 Otherwise use of works would be very restricted in practice. A user may for example

Whether authors should be able to transfer their right of attribution is a delicate matter. On the one hand, an author may be part of a collective desiring to publish a work as a unified entity. Here, I believe transferring the right of attribution is justified. On the other hand, there are instances where an author may want to transfer a work to some person who is disconnected from the production of the work. In this second case I see transfer as illegitimate, principally because of the public's interest in not being deceived about who produced a given work. The difficulty consists in these two cases not always being easily distinguishable.

Non-endorsement: authors have the right of having it clearly stated that a use or modification of their work is not endorsed or approved by them.

People who use others' authorial creations must make it clear that their use does not necessarily signify endorsement by the original author. Otherwise it might be thought that the uses or modifications undertaken were approved by the original author, and this can illegitimately reflect back on them. This right complements the right of attribution and protects authors' correct social recognition. This right should have no impact on the public's ability to use a work. A user does not even need to know a work's author in order to include a notice saying its author does not necessarily endorse her use of it. Indeed, if it were generally known that use of a work does not imply endorsement, including such notices might become unnecessary.

Profit sharing: authors have the right to a fair share of the profits made from commercial exploitation of their works.

Profit sharing has the potential of benefiting authors without damaging public interest. The share of the profits given to authors should be such that commercial use is not unduly restricted and non-commercial use not affected at all[13]. To ensure that authors cannot unduly leverage this principle, the share should not be subject to negotiations between the author and

be unable to locate the author of a work because the necessary records do not exist or are very difficult to access. Works can also be based on so many prior works that it becomes infeasible to attribute them all.

13 I gloss over a significant difficulty here insofar as it is not always easy to distinguish commercial from non-commercial uses.

the commercial user but set beforehand by a competent institution. Such a profit sharing rule should incentivise the production of authorial works without negatively impacting the public's ability to use, modify, and share authorial works. This right is also in the interests of authors. They gain an additional means of income and recognition, and their works are protected from being used to the exclusive financial benefit of others.

For how long should we protect the three rights I have described so far? I do not know. I believe this matter depends on the structure of the overall legal system, on the economic situation and system, and other factors. I do not however believe that the protection should ever be longer than the life of the author. Authors' personality interests extinguish with their deaths, and it is dubious whether longer-than-life terms of protection provide any additional incentives to authors.

Alternative compensation systems: authors should be fairly compensated for their work.

Profit sharing alone might not be able to provide sufficient financial incentives to authors. Moreover, authors should be compensated for their contributions to society and given the means necessary to lead decent lives. At least the latter two of these matters are not specific to authors; they are concerns about fairness and social justice, which apply to everyone. When designing alternative compensation systems, care should be taken to ensure they fulfil their twin goals of providing financial incentives and enabling a decent life for authors.

I believe these four principles suffice. Additional economic rights are unwarranted from a public interest perspective if authors' income and financial incentives are guaranteed by profit sharing and alternative compensation systems and if such rights negatively affect public interests. I believe this is the case at least for all the classical economic rights. From a personality interest perspective, Radin (1982) has argued that property rights are a means of recognising authors for their important contributions. Not giving this point the discussion it deserves, I will only state that I think there are more valuable forms of recognition that we should espouse instead.

Possible additional moral rights require a more detailed discussion. Authors may, for example, be associated with uses of their works even when a non-endorsement notice is included. This risk is real; however, the danger

is minor and no worse than in the copyright system. Firstly, most people should take a non-endorsement clause at face value. Secondly, the danger of an author's unjustified association with uses of her work diminishes when authors have less control over their works. When authors have a high level of control over their works, not exercising their rights can more plausibly be interpreted as endorsement as when authors lack any ability to control their works. Thirdly, copyright itself can not ensure that an author is never unjustifiably associated with uses of her works. One cannot prohibit people from thinking certain thoughts, and there always exists the possibility of some people making unjustified associations between authors and uses of their works. Finally, it is not always unjustified to associate an author against her will with a certain use of her work.

An author may also feel that she loses her ability to express herself when others use her creations in ways she dislikes or even abhors. This may stop her from trying to publicly express herself, which can endanger her capacity for self-actualisation. Sometimes this situation is conceived of as a conflict between competing personality interests: on the one hand there is the author and on the other the user who tries to give the work a new meaning. Yet, such a conflict is not necessary as is evidenced by the many authors who renounce the right to control their creations and who indeed see this as furthering their personality interests[14]. I believe whether or not authors are hurt in this sense by certain uses of their works depends on the attitudes they have towards their works. If an author does not believe she owns the work in question, if she understands that she's not the sole source of its meaning, if she is tolerant of other views, and if she sees authorial works as building on a cultural commons, then uses she dislikes are less likely to endanger her quests for self-actualisation.

Authorial works created by others play important roles in our lives and are often integral to our personality development. Many of us have prob-

14 One example is the importance given by the *hacker ethics* to not restricting access to works and information. This is a fundamental part of the hacker identity (Chaos Computer Club, 2016) and evidenced by *Free Software*. Another example are the hugely popular *Creative Commons* licenses with which authors can forgo most of the rights accorded by copyright. For instance Flickr, an image hosting website, holds 350 million photos with such a license ('Creative Commons. Flickr', 2016).

ably been significantly influenced by some of the books we read, and it is not uncommon for this influence to be so strong that it helps define who we are. A person may want to share with others works they feel express their personalities. In other cases, authorial works need to be adapted to best suit the individual's expressive desires. Both modification and distribution may however not be possible since copyright per default prohibits such uses. Copyright protection therefore often negatively impacts others' ability for self-actualisation and «systemically prevent[s] prospective personhood interests from *developing*" (emphasis in the original) (Hughes, 1998).

Forms of authorial self-actualisation that build on copyright and thus endanger others' quests for self-actualisation can also be seen as noxious and not morally valuable. If this is correct, hurting the public would also be harmful to authorial personality interests. Radin (1982) for example argues that appropriation is "healthy" – conducive to valuable self-actualisation – only in those instances where it does not harm others. And in the case of copyright, harming others cannot be escaped without renouncing one's rights, at least as long as some rights cannot be acquired or some people lack the necessary financial means therefor.

Both public interest and personality interest accounts show that copyright necessarily has negative effects on the public, whereas the effects on authors are neither inevitable nor clearly positive or negative in character. I have also argued that the possible negative effects on authors, stemming from unauthorised use or modification of their works, depend on their attitudes towards their works. Renouncing the control over one's works can even constitute a valuable part of authorial personality. Therefore, if it is possible to change authors' attitudes towards their creations – which I believe it is – then it is better to bring about such a change than to insist that the public must be harmed.

7. Contributors

Until now I have analysed two types of interests: authorial interests and public interests. These two do not however exhaust all the possible moral interests people have in authorial works. In this section I explore interests of contributors – people who are not authors but more involved in the production of works than the public.

Copyright has a place for at least some contributors. If I contribute a paragraph to a novel, the novel's author does not hold the copyright in the paragraph in question; this copyright is mine. She instead holds the copyright in the creative ordering of the different parts of the book as well as in those parts of the book she authored.

Not every type of contribution benefits from copyright protection. Firstly, some contributions are considered too insubstantial or too small to be protected (Colston, 1999). Secondly, and more importantly, there are contributions that are far from insubstantial that also lack protection. For instance, film directors usually obtain the copyright and moral rights in a film, even though there are many others whose contribution is far from negligibly small. Another example is the master craftsman who fashions a statue according to an artist's plans and who does not profit from any copyright protection either.

It could now be argued that these contributors do not make the cut because they lack creativity – they merely implement another person's creative idea. While the truth of this is questionable, protecting contributors does not even require them to be creative. The various approaches that failed to ground copyright because they applied not only to authors might justify interests for contributors. It might for example be argued that the effort that contributors expend gives rise to moral interests. It might also be reasoned that contributors are justified to personally identify with the creation of others' authorial works because they have intentionality personality interests in the work. These personality interests are connected to our intentional actions and their importance for a person's sense of agency (Hughes, 1998).

We have seen in earlier sections that personal input and thus creativity are a matter of degree, and it is therefore difficult to argue why there should be a concrete cut off point below which no rights at all should be accorded. The difference between authorial and contributors' interests is one of degree. It is very difficult to say when a contribution becomes sufficiently creative to merit being called an authorial work on its own. This leads me to agree with Hilpinen who argues that it is «possible to distinguish degrees of authorship» (emphasis original) (Hilpinen, 2011, sec. 4). These degrees of authorship could then be accompanied by degrees of rights.

Would the existence of contributors' moral interests imply that we

should extend the range of people to whom copyright is accorded? I do not think so for a simple reason, which I will not however flesh out here: contributors' personality interests are likely to be less strong than authors' and according copyright to contributors could harm the general public by further complicating the legal situation. Therefore, if authors' should only be granted very limited exclusive rights, then the case is even more clear-cut with contributors.

I believe contributors' interests could lead us to espouse new ways of attribution that give recognition also to those who are now invisible. One interesting approach can be seen in *Free Software* projects, which are often hosted on platforms – *Version Control Systems* – that record all the changes made to the source code. Every contribution is publicly recorded and usually attributable to a specific person. One can easily find out whether a specific contribution is substantial or not and appraise its value. By attributing every contribution, such systems render it less important who is an author and who a contributor, stressing instead the collective nature of creativity.

8. Conclusion

Valid authorial and public interests in authorial works exist. However, Lockean approaches cannot even in principle justify exclusive authors' rights. While consequentialist as well as personality interest theories can do so, they also fail to justify copyright. What consequentialism and personality interests do justify is the limited set of rights I have presented towards the end of this paper. In addition, I have argued that we might need to think of ways to protect the interests of contributors.

This paper has tried to present an overall view of the ethics of copyright. I have done so because I believe only a pluralist account can allow for judgements on copyright's moral status. Unfortunately this meant leaving by the wayside many of the details of the argument. A first inadequacy is that the moral foundations grounding the interests I have argued for were to a large extent absent. How exactly are authorial works important for self-actualisation? What values should a consequentialist account take into consideration? I have also mentioned the importance of authors' attitudes towards their works without giving this much thought. Virtue ethics, which I have also ignored, might help in investigating the attitudes authors should

hold towards their works (see Benkler and Nissenbaum, 2006). This last point deserves emphasis: we need more research on the nature and value of the relationship between authors and their works.

I also had to leave aside many additional arguments in favour of my view on copyright. Above all, the rich literature on the value of the commons and of collaborative creative processes comes to mind. In general, my paper has focused perhaps too heavily on the individual, disregarding to what extent culture and knowledge production are social processes.

My analysis has focused on copyright law. A more complete investigation of the ethics of authorial works would have to cover additional questions. Not all of the moral issues surrounding authorial works are codified and these non-legal areas would need to be considered, too. I have also not treated the question of when authors should – or must – publish works or refrain from doing so. Finally, copyright interrelates with other spheres of intellectual property–patents and trade marks–and these interrelations deserve to be analysed.

I hope to see more, and more expansive, pluralist analyses of the ethics of authorial works. The significance of copyright can hardly be understated as it shapes one of the defining aspects of our humanity: our culture. Given these stakes, I have no doubt that copyright will remain a domain of heated debates for many years to come. We need more than that however – we need honest efforts at mutual understanding and constructive criticism. My hope is that moral philosophers will help making this extremely important discussion a fruitful one.

9. References

1. Abbott, F. M., Cottier, T. and Gurry, F. (2011). *International Intellectual Property in an Integrated World Economy*. 2nd ed. Aspen Casebook Series. New York, NY: Wolters Kluwer Law & Business.
2. Aigrain, P. (2012). *Sharing: Culture and the Economy in the Internet Age*. Amsterdam, NL: Amsterdam University Press.
3. Benkler, Y., and Nissenbaum, H. (2006). 'Commons-Based Peer Production and Virtue'. *Journal of Political Philosophy* 14(4), pp. 394–419.
4. Chaos Computer Club (2016). 'Hackerethik. CCC'. Accessed January 11. **https://www.ccc.de/de/hackerethik**.

5. Colston, C. (1999). *Principles of Intellectual Property Law*. London, UK: Cavendish.
6. 'Creative Commons. Flickr' (2016). Accessed January 11. **https://secure.flickr.com/creativecommons/**.
7. Dewey, J. (1980). *Art as Experience*. New York, NY: Perigee Books.
8. DiCola, P. (2013). 'Money from Music: Survey Evidence on Musicians' Revenue and Lessons About Copyright Incentives'. *Arizona Law Review* 55, p. 301.
9. Douglas, G., Mitra, A., Gupta, N., and Shaw, J. D. (1998). 'Are Financial Incentives Related to Performance? A Meta-Analytic Review of Empirical Research'. *Journal of Applied Psychology* 83(5), pp. 777–87.
10. Dutfield, G. (2008). *Global Intellectual Property Law*. Cheltenham, UK; Northampton, MA: Edward Elgar.
11. Fisher, W. (2007). 'Theories of Intellectual Property'. In *New Essays in the Legal and Political Theory of Property*, pp. 168–99. Cambridge, UK; New York, NY: Cambridge University Press.
12. Gillespie, T. (2007). *Wired Shut: Copyright and the Shape of Digital Culture*. Cambridge, MA: MIT Press.
13. Hilpinen, R. (2011). 'Artifact'. In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Winter 2011.
14. Himma, K. E. (2008). 'The Justification of Intellectual Property: Contemporary Philosophical Disputes'. *Journal of the American Society for Information Science and Technology* 59(7), pp. 1143–61.
15. Hughes, J. (1988). 'The Philosophy of Intellectual Property'. 77 *Georgetown Law Journal* 77, pp. 287-366.
16. ——— (1998). 'The Personality Interest of Artists and Inventors in Intellectual Property'. *Cardozo Arts & Entertainment Law Journal* 16, pp. 81–181.
17. Kravets, D. (2008). 'File Sharing Lawsuits at a Crossroads, After 5 Years of RIAA Litigation'. Wired: Threat Level. **http://www.wired.com/2008/09/proving-file-sh/.**
18. Liebowitz, S. J., and Watt, R. (2006). 'How to Best Ensure Remuneration for Creators in the Market for Music? Copyright and Its Alternatives'. *Journal of Economic Surveys* 20(4), pp. 513–45.

19. Locke, J. (1764). *Two Treatises of Government*. Edited by Thomas Hollis. London, UK: A. Millar et al.
20. Lucibella, C. (2010). 'Filesharing and Ownership of Digital Objects: Intellectual Property According to Kant's Theory of Possession.' *Theoretical and Applied Ethics* 1(1), pp. 35–40.
21. Moore, A. (2008). 'Personality-Based, Rule-Utilitarian, and Lockean Justifications of Intellectual Property'. In *The Handbook of Information and Computer Ethics*, edited by Kenneth Einar Himma and Herman Tavani, 105–30. Hoboken, NJ: Wiley.
22. ——— (2011). 'Intellectual Property'. In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Summer 2011.
23. Murphy, D. J. (2012). 'Are Intellectual Property Rights Compatible with Rawlsian Principles of Justice?' *Ethics and Information Technology* 14(2), 109–21.
24. Nein (2013). 'Another Beautiful Day for the Culture Industry. for Culture, Not so Much. @NeinQuarterly'. Microblog. August 31. **https://twitter.com/NeinQuarterly/status/373772028069044224.**
25. Nozick, R. (1974). *Anarchy, State, and Utopia*. Oxford, UK: Blackwell.
26. Radin, M. J. (1982). 'Property and Personhood'. *Stanford Law Review* 34(5), pp. 957–1015.
27. Rawls, J. 2000. *Lectures on the History of Moral Philosophy*. Edited by Barbara Herman. Cambridge, MA: Harvard University Press.
28. Resnik, D. B. (2003). 'A Pluralistic Account of Intellectual Property'. *Journal of Business Ethics* 46(4), pp. 319–35.
29. Ryan, R. M., and Deci, E. L. (2000). 'Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions'. *Contemporary Educational Psychology* 25(1), pp. 54–67.
30. Spinello, R. A. (2003). 'The Future of Intellectual Property'. *Ethics and Information Technology* 5(1), pp. 1–16.
31. Spinello, R. A., and Bottis, M. (2009). *A Defense of Intellectual Property Rights*. Cheltenham, UK; Northampton, MA: Edward Elgar

The concept of intellectual property: From Plato's Views to Current Copyright Protection in the Light of Open Access

by Nikos Koutras[1]

1. Introduction

This paper argues that Plato's rationale about the concept of property and its communal framework of sharing through joint ownership is more persuasive than others, as it justifies the philosophy of open access. The origins of the notion of property lie in Plato's philosophy. In accordance with Plato's ideas, the concept of property was first introduced as comprising joint ownership (in terms of social justice) and being a beneficial tool that could support the growth of the ideal republic. Plato argued that private property should not exist and property should fall under the 'umbrella' of joint ownership to ensure peace and justice. Aristotle consequently adopted his teacher's notions in relation to property but focused on a more individualistic aspect of property. Aristotle indicated his disagreement with Plato's rationale for joint ownership by asserting that such extreme unification was against the diversity of personal identity and would affect the benefits derived from market exchanges.

In addition, this paper also argues that Locke's philosophy extended the concept of private property ownership. Locke asserted that whatever work is produced by an individual becomes her property. He used this premise to make a connection between ownership and creation. The period in which Locke wrote represents a shift in the concept of property, as goods went from being viewed as private property to a form of creative effort. In his work entitled the 'Second Treatise on Government', Locke sought to find the right by which an individual can claim to own one part of the world when, according to the Bible, God gave the world to human beings

1 PhD, PhD (cand.), Macquarie University, Political Scientist, IP tutor.

in common. In answer to this question, Locke argued that individuals own themselves and, thus, own the fruits of their own labours. On this point, a connection can be seen between Aristotle and Locke's logic; they both agree that the issue of private property is one of the numerous intricacies. However, Locke took a more individualistic approach to property ownership than Aristotle.

Conversely, Hegel contended that property should be understood as a phase in the growth of humankind and personality. Hegel adopted Aristotle's and Locke's logic and reasoning to extend the appropriate environment and surroundings of property. A consideration of these philosophers' arguments in their chronological order and, more specifically, their flow of thinking led me to propose a justification for the emergence of open access as an additional support to current copyright regimes.

From the time of Aristotle to modern times, differences can be seen in how the traits of property have been conceptualised. One by one, philosophers have added new features to the concept. Plato's basic argument of joint ownership and the communal property has often been neglected. Plato's arguments in relation to communal property and joint ownership form a substantial part of the justifications for my argument and the significance of these arguments in relation to open access must be considered. Accordingly, the argument of this paper is subliminally based on Plato's logic and his notions about the communal use of property, as they highlight several, unique aspects of communities and individuals.[2]

In modern times, when information and communication technologies are a real revolution, it is necessary to return to Plato's concepts to argue that open access is an instrument that benefits the wide dissemination of information resources. Thus, the paper argues that the emergence of property as a concept requires copyright protection to be considered in the context of open access. This paper presents justifications for the introduction of private property and discusses how the idea of private property (i.e., land

2 This mutual philosophical consideration is best described as follows: Aristotle highlighted individualism and self-interest Locke asserted that property rights represent an individual's natural rights. Hegel asserted that all type of individual's rights lie in property; Hohfeld outlined eight different relations that stem from property as a right; and Honoré, lastly, considered property as an account of ownership rights.

and goods) was extended to intellectual creations. All in all, the concept of open access represents an additional means of support for the existing copyright framework of protection in the digital age by enabling information to be distributed and accessed, legally.

2. The first introduction of property as a concept

2.1 Plato's philosophy

Plato's ideas on property were related to his ideas about family, society and the republic. They also contained the origins of patents. In Ancient Greece (around 500 B.C.), the Greek city of Sybaris recognised a form of patent rights for the creation of unique culinary dishes.[3] These rights encouraged individuals to discover new refinements in luxury, as any profits derived from these discoveries were secured to the inventor for one year.[4] Thus, creative endeavours were encouraged in Ancient Greece; however, the one-year limitation also protected the market from monopolies or economic advantages being held by few citizens of the republic or society. Plato's ideas describe an ideal republic in which philosophers share common property in terms of justice.[5] Plato argued for joint ownership system[6] forms a fundamental element for justice and provides the basis for the 'ideal republic'.[7] In this period, we can see the first justification for extending the notion of private property in goods (i.e., culinary dishes) to creative endeavours (i.e. patent protection for one year) can be seen.

Another aspect that stems from Plato's ideas is that of wealth and private property. The abolishment of wealth leads directly to the decay of the

3 Anthony Rich, *A Dictionary of Roman and Greek Antiquities* (Nabu Press, 2010).

4 William Smith, *A Concise Dictionary of Greek And Roman Antiquities* (Nabu Press, 2010).

5 Charles H. Kahn, *Plato and the Socratic Dialogue: The Philosophical Use of a Literary Form* (Cambridge University Press, 1998).

6 Michael Shalom Kochin, *Gender and Rhetoric in Plato's Political Thought* (Cambridge University Press, 2002).

7 Leon H. Craig, *The War Lover: A Study of Plato's Republic* (University of Toronto Press, 1996); Stanley Rosen, *Plato's Republic: A Study* (Yale University Press, 2005); Jonathan Lear, 'Allegory and Myth in Plato's Republic' in Gerasimos Santas (ed), *The Blackwell Guide to Plato's Republic* (Blackwell Publishing, 2006) 25.

traditional family. Plato also argued that there should be no legacies, private property or nepotism, as these create negative inherent idioms for the whole society.[8] By providing a form of protection to the creators of culinary dishes, Plato's original idea for property as existing in goods was extended to creative endeavours via a form of patent protection. Legacies and private property do not only consist of tangible objects; this is especially true today. An intellectual creation can comprise a legacy for the public domain and society as a whole.

Plato argued that owning private property creates greed and lust. This argument led to some people calling Plato a proto-socialist or proto-communist. However, Plato only made this argument in relation to the guardian class and auxiliaries to focus their attention on the ever-important matter of the state. This argument also represents the first time that someone initiated a discussion on the importance of private property, its content, how it was going to be used and the main purposes for owning property.[9]

According to Plato, property was affiliated with the concept of family and, particularly, 'children'. Plato argued that having a child creates greed and lust. Plato asserted that children should be taken from their biological parents and redistributed by the state to other parents. This is also how he supported his arguments concerning private property and the right to 'own' a child.[10] Thus, Plato did not believe in private property as such and ultimately argued that no one, except philosophers, should own anything.[11] Plato influenced his student Aristotle, just as Socrates had influenced Plato. However, each man's influence evolved differently. Plato believed that concepts, such as property, have a universal or ideal form that leads to an idealistic philosophy and ideal republic. Conversely, Aristotle believed that universal forms could not appropriately be attached to objects or concepts and thus each object or a concept must be examined on its own. Plato was more interested in justifying a form of communism among the elites based on

8 J. Angelo Corlett, *Interpreting Plato's Dialogues* (Parmenides Publishing, 2005) vol 47.

9 Press, above n 8, 135.

10 Catherine H. Zuckert, *Plato's Philosophers: The Coherence of the Dialogues* (University of Chicago Press, 2009).

11 Coleen Zoller, 'Interpreting Plato's Dialogues (Review)' (2007) 45 *Journal of the History of Philosophy* 486.

joint ownership whereas Aristotle sought to justify a political order based on private property from the individual aspect. Such differences in logic led me to examine Aristotle's views on the concept of property.

2.2 Aristotle's philosophy

A compelling Aristotle put forth the argument in favour of private property.[12] Perhaps influenced by the private property arguments of another Greek philosopher, Democritus, Aristotle delivered a cogent argument for the communisation of the ruling class as originally called for by Plato.[13] However, he denounced Plato's goal for the perfect unity of the state through communism, pointing out that such extreme unity runs against the diversity of mankind and the reciprocal advantage that can be reaped through market exchange.[14]

Aristotle delivered a point-by-point comparison of private and communal property.[15] First, he argued that private property is more productive than communal property and will lead to personal growth. It appears that Aristotle connected creation and production with progress and saw the need to extend Plato's idea about property to encompass goods to creative endeavours. According to Aristotle, goods owned in common by a large number of people receive little care, as people mainly focus on their own self-interests;[16] however, people will show greater interest and care their

12 Emily Brady, 'Aristotle, Adam Smith and the Virtue of Propriety' (2010) 8 *Journal of Scottish Philosophy* 79; Martin J. Calkins and Patricia H Werhane, 'Adam Smith, Aristotle, and the Virtues of Commerce' (1998) 32 *The Journal of Value Inquiry* 43.

13 Henry William Spiegel, *The Growth of Economic Thought* (Duke University Press, 1991); Jacques Brunschwig, *A Guide to Greek Thought: Major Figures and Trends* (Harvard University Press, 2003); Lawrence Nolan, *Primary and Secondary Qualities: The Historical and Ongoing Debate* (Oxford University Press, 2011).

14 Allan David Bloom, *The Republic of Plato* (Basic Books, 1991); Robert Mayhew, *Aristotle's Criticism of Plato's Republic* (Rowman and Littlefield Publishers, 1997)

15 Elinor Ostrom and Charlotte Hess, 'Private and Common Property Rights' (SSRN Scholarly Paper ID 1936062, 29 November 2007) *Social Science Research Network*, <http://papers.ssrn.com/abstract=1936062>.

16 Colin Ash, 'Social Self-Interest' (2000) 71 *Annals of Public and Cooperative Economics* 261; Ian Maitland, 'The Human Face of Self-Interest' (2002) 38 *Journal of Business Ethics* 3; Samantha Besson and José Luis Martí, *Deliberative Democracy and its Discon-*

own private property.

Secondly, Plato argued that common property is conducive to social peace, as no one will be envious of, or able to take, the property of another. Conversely, Aristotle argued that common property would be a continuing and intense source of conflict as individuals will complain that they have worked harder and obtained less than others who have done little and taken more from the common store. Further, Aristotle noted that not all crimes or revolutions are powered by economic motives. As Aristotle trenchantly stated: 'men do not become tyrants in order that they may not suffer cold' (p. 25).[17] In interpreting Aristotle's statements, it is clear that the work and contribution of creators to society have to be awarded and protected. Under this rationale, it is imperative to create an appropriate form to protect intellectual creations. Plato's views about the concept of common property creates negative aspects that could easily cause injustice and conflict in relation to creators' profits.[18] Thus, Aristotle provided a justification for transforming Plato's argument for the concept of property and expanded it from encompassing private property in goods to private property in creative efforts.

Thirdly, private property is plainly embedded in man's essence. An individual's admiration of personality, individuality, money and property are interconnected in a natural love of exclusive ownership. Fourthly, Aristotle noted that private property has existed always and everywhere.[19] To enforce a system of communal property on societies would be to disregard the record of human experience to leap into the new and untried. Ultimately, it appears that abolishing private property would create more problems than

tents (Ashgate Publishing, 2006); Hector O' Rocha and Sumantra Ghoshal, 'Beyond Self-Interest Revisited' (2006) 43 *Journal of Management Studies* 585; Carsten K.W. de Dreu and Aukje Nauta, 'Self-Interest and Other-Orientation in Organizational Behavior: Implications for Job Performance, Prosocial Behavior, and Personal Initiative' (2009) 94 *Journal of Applied Psychology* 913.

17 Eugene Garver, *Aristotle's Politics: Living Well and Living Together/Eugene Garver.* University of Chicago Press, 2011.

18 Hans-Hermann Hoppe, *The Ethics and Economics of Private Property* (11 October 2004) Mises Institute <http://mises.org/library/ethics-and-economics-private-property>.

19 Murray N. Rothbard, *Aristotle on Private Property and Money* (30 November 2009) Mises Institute <http://mises.org/library/aristotle-private-property-and-money>.

it would solve.

Aristotle wove together his economic and moral theories to reach the brilliant insight that private property furnishes individuals with opportunities to act morally, (e.g. to practice the virtues of welfare and charity). The compulsory communal property would destroy these opportunities. Thus, in accordance with Aristotle's philosophy, the concept of private property constitutes a means of wealth, production and justice and should be protected.

Aristotle was critical of moneymaking;[20] however, he still opposed any limitation being placed on an individual's right to accumulate private property. He contented that education should teach individuals how to voluntarily curb their rampant desires and lead them to limit their own accumulations of wealth. Despite his cogent defence of private property and opposition to coerced limits on wealth, as an aristocrat, Aristotle was as scornful of labour and trade as his predecessors.

Aristotle raised many issues by morally condemning the lending of money[21] for interest as 'unnatural'.[22] Aristotle contended that as money cannot be used directly, but is employed only to facilitate exchanges, it is 'barren' and should not be used to increase wealth. Thus, Aristotle incorrectly viewed the charging of interest as money production and condemned it as being contrary to nature. As Plato's student, Aristotle pursued his teacher's view on the issue of private property, but, ultimately, took an opposite point of view. After repeatedly rejecting Plato's ideal state as a dream that would never eventuate, Aristotle took a stand in favour of private property.[23] He believed that owning private property was necessary to the stability of the

20 Scott Meikle, *Aristotle's Economic Thought* (OUP Catalogue, Oxford University Press, 1997) <https://ideas.repec.org/b/oxp/obooks/9780198152255.html>; Harvey C. Mansfield Jr., 'Marx on Aristotle: Freedom, Money, and Politics' (1980) 34 *The Review of Metaphysics* 351; Stephen Zarlenga, 'The Lost Science of Money' (2004) 16 *European Business Review* <http://www.emeraldinsight.com/doi/abs/10.1108/ebr.2004.05416eab.004>.

21 Irene van Staveren, *The Values of Economics: An Aristotelian Perspective* (Routledge, 2013).

22 Richard Kraut and Steven Skultety, *Aristotle's Politics: Critical Essays* (Rowman and Littlefield, 2005).

23 Mary Louise Gill and Pierre Pellegrin, *A Companion to Ancient Philosophy* (John Wiley and Sons, 2009).

state, especially if everyone owned a moderate and sufficient amount of property.

When Locke's political theory was first printed in 1689, the impressive authority of Aristotle stood ready to defeat it. However, when it was confirmed that the renowned author of *An Essay Concerning Human Understanding* had also written the anonymously published *Two Treatises of Government*, Locke was broadly viewed as having put forward a distinctive political theory based on individual rights and social contract; an approach to politics that has often been attributed to Aristotle. The classical philosophy of Aristotle was in due course followed by the development of a liberal philosophy. Locke is one of the foremost liberal thinkers and his ideas on property inform our contemporary understandings. Thus, I will now analyse the concept of private property in relation to Locke's ideas on the property.

3. The introduction of private property: from lands and goods to intellectual efforts

3.1 Locke's philosophy on property

Locke and Aristotle agreed that the issue of private property is one of numerous intricacies. However, both philosophers held disparate views on the distribution of land among individuals. Locke took a more individualistic approach to property ownership than Aristotle. In the *Second Treatise on Government*,[24] Locke sought to ascertain the right by which an individual can claim to own one part of the world when, according to the Bible, God gave the world to human beings in common. In his work, Locke argued that individuals own themselves and their own labour; thus, individual property rights are natural rights. This approach was similar Aristotle's approach (who, as stated above, did not support Plato's arguments for joint ownership).

24 Jonathan Bennett, 'Second Treatise of Government-John Locke' <http://www.early-moderntexts.com/pdfs/locke1689a.pdf>; John Locke, *Two Treatises of Government* (CreateSpace Independent Publishing Platform, 2013); John Locke, *Second Treatise of Government: An Essay Concerning the True Original, Extent and End of Civil Government* (John Wiley & Sons, 2014).

Adopting this line of thought, when an individual's work (relevant to the outcome of the work) manifests in tangible objects it becomes the property of the individual. Political philosopher Nozick calls this idea a Lockean proviso. According to Locke, labourers must hold a natural property right in the resource itself as the ownership was an appropriate component of production. Additionally, Locke asserted that a preceding natural right interconnects property and ownership with production; thus, the concept of property includes exclusive rights on tangible ideas, especially those produced through creative endeavours. Aristotle and Locke disagreed on many issues in relation to property ownership, including acquisition, maintenance and divine intervention. However, it should be emphasized that there are several issues in relation to property rights on which these two philosophers agreed, including the issue of equity.

Locke's theory on property can be viewed as an expansion of Aristotle's main argument in relation to private property. Locke argued that individuals could acquire full property rights over moveable and non-moveable parts of the earth in a state of nature. The terms moveable and non-moveable represent tangible and intangible ideas (e.g. notions, innovations, thoughts and intellectual creations). Locke's contribution to property theory expanded Aristotle's concept. Locke stated that every individual has his own property to which nobody else has any right. However, unlike Locke, Aristotle argued that owners of private property should share it. Locke revised Aristotle's ideas about sharing and argued that individuals should only acquire as much property as appropriate and should not acquire property in an endless manner. Thus, Locke developed Aristotle's concept of property and provided justifications the application of the principle of private property in goods to creative endeavours. Hegel further developed Locke's ideas in relation to property by transforming them into a natural right and his philosophy is considered below.

3.2 Hegel's philosophy

There exist several approaches and different definitions of property; however, each of these definitions has a common element: each definition treats property as a means rather than an end. Property can be viewed as a means

to a 'good life', as a means to gain freedom or social recognition.[25] Hegel followed Locke's rationale in respect of the relationship between individuals and property, arguing that property is the embodiment of personality. Hegel's arguments can be seen as extending Locke's notions in relation to private property, as he claims that property is the embodiment of personality and, in this way, it is transformed into a natural right.

Additionally, Hegel argued that the basis of individuals' rights lies in property. Hegel followed the same logic as Locke and noted that, despite being central to an individual's assertion of identity and personality, property does not merely represent a material acquisition. Thus, according to Hegel, property comprises both material and non-material aspects (i.e. tangible and intangible ideas). By describing private ownership as an aspect of self-interest, Aristotle encouraged philosophers like Locke and Hegel to further develop the argument that property rights are natural rights and embody personal growth. Thus, individuals' notions and self-interests are inherently distinguishable from intellectual creations. This philosophical concern suggests that intellectual creations should be secured and protected to ensure that the concept of property moves from goods to intellectual creations.

According to Hegel, property is an expression of ourselves and represents the 'location', room or space where an individual is able to assert his or her rights (respected by others) and state that 'this is mine'.[26] The system of private property establishes individuality *via* contract and exchange. Hegel used this point to justify the inevitable links among property, personality growth and profits stemming from self-interest. Contracts demonstrate ownership through institutionalised patterns of mutual respect of the rights and commitments of individuals. Economic life, governed by a free

25 Margaret Jane Radin, *Reinterpreting Property* (University of Chicago Press, 1993); D.B. Resnik, 'A Pluralistic Account of Intellectual Property' (2003) 46 *Journal of Business Ethics* 319; Christopher May, *The Global Political Economy of Intellectual Property Rights: The New Enclosures?* (Routledge, 2013).

26 Dudley Knowles, 'Hegel on Property and Personality' (1983) 33 *The Philosophical Quarterly* 45; Michael Salter, 'Justifying Private Property Rights: A Message from Hegel's Jurisprudential Writings' (1987) 7 *Legal Studies* 245; Hans-Christoph Schmidt am Busch, 'Personal Respect, Private Property, and Market Economy: What Critical Theory Can Learn from Hegel' (2008) 11 *Ethical Theory and Moral Practice* 573.

exchange of goods, is based on an institutionalised notion that the individual has some claim to recognition as a right-bearing person. For exchange markets to operate effectively, economic actors have to identify universal standards by which individuals can claim to own property. Established patterns of mutual recognition in the modern economic sphere are embodied in economic actors and depict a 'common will'.[27]

Consequently, an individual has no particular traits or reference to a social environment. Thus, under Hegel's idea of private property, rights are abstract and individuals are engaged as universal subjects without specific features.[28] Hegel also introduced morality to the concept by combining the system of mutual recognition and abstract rights; for example, morality represents the subjective part of mutual social commitments institutionalised in contracts and the economic market. Moreover, individuals observe these commitments as moral obligations. Therefore, they respect intellectual rights as an ideal good based on mutual recognition.

In accordance with Hegel's philosophy that emphasises human needs, property is the first component of freedom and a substantial purpose. On this point, Hegel stated that if possession (i.e., the power over items) is simply pursued to satisfy self-interest then it provides a means to satisfy these types of need. However, according to Hegel, human satisfaction is the attempt to bring to an agreement that recognises the subject of free agency. In this manner, power over items is a means for the growth of individual personalities. Thus, this justification demonstrates the importance

27 J. Rogers Hollingsworth and Robert Boyer, *Contemporary Capitalism: The Embeddedness of Institutions* (Cambridge University Press, 1997); Christoph Knill and Dirk Lehmkuhl, 'Private Actors and the State: Internationalization and Changing Patterns of Governance' (2002) 15 *Governance* 41; Kalypso Nicolaidis and Gregory Shaffer, 'Transnational Mutual Recognition Regimes: Governance without Global Government' (2005) 68 *Law and Contemporary Problems* 263; Wenchao Zhang et al, 'Local Gabor Binary Patterns Based on Mutual Information for Face Recognition' (2007) 7 *International Journal of Image and Graphics* 777; Caifeng Shan, Shaogang Gong and Peter W McOwan, 'Facial Expression Recognition Based on Local Binary Patterns: A Comprehensive Study' (2009) 27 *Image and Vision Computing* 803.

28 George Wilhelm Fredrich Hegel, *Hegel: Elements of the Philosophy of Right* (Cambridge University Press, 1991); Russell Cropanzano et al. 'Self-Enhancement Biases, Laboratory Experiments, George Wilhelm Friedrich Hegel, and the Increasingly Crowded World of Organizational Justice' (2001) 58 *Journal of Vocational Behavior* 260.

of an effective interconnection among self-interest, property and personal progress or individual advancement.

Hegel claimed that property is the manifestation of an individual's effort to deploy his or her powers and become self-consciousness by the appropriation of his or her environment.[29] Consequently, Hegel task was not to provide a justification for property but to comprehend and understand it as a phase in the process of intellectual production. Hegel did not make any effort to justify property in the context of Plato's ideas in relation to joint ownership. Indeed, he ignored the role of property in the growth of an individual's self-awareness. Intellectual property demonstrates individuals' thoughts, ideas, notions and ways of thinking. Thus, it is necessary to clarify whether individuals participate in a process whereby their notions or thoughts are developed in accordance with their subliminal willingness. This statement supports Hegel's understanding of property as a phase in the process of human mind production.

To support my argument, I briefly explained Hegel's theory of property. Hegel showed that in relation to self-interest, private property exists in either tangible or intangible objects that should be protected, as property 'participates' in the process of human mind production. Thus, it is evident that the ideas and notions of Plato, Aristotle, Locke and Hegel on the concept of property developed from a consideration of communal ownership to individual ownership. Further, their justifications for ownership expanded the concept of property from physical to intellectual goods. The concept of private property as a natural right gradually lent itself a number of notions that reflected the elements of such a right.

3.3 Hohfeld's philosophy

Since Hegel first argued that property was a natural right, many other philosophers have elaborated on what a natural right in property means. Perhaps, the most notable forerunner in this respect was Wesley Hohfeld

29 Richard Teichgraeber, 'Hegel on Property and Poverty' (1977) 38 *Journal of the History of Ideas* 47, 47; Stephen R. Munzer, *A Theory of Property* (Cambridge University Press, 1990); Jeanne L Schroeder, 'Unnatural Rights: Hegel and Intellectual Property' (2005) 60 *University of Miami Law Review* 453, 453–456; May, above n. 24, 45–47.

whose theory comprised eight legal relations.[30] Hohfeld further developed and clarified the meaning of property as a right. In the following discussion, Hohfeld's ideas in relation to property rights are explained, as they inform the bundle theory, a legacy of legal realism.[31] The origins of bundle theory can be traced back to late 19th century and early 20th century analytical jurisprudence.[32] Hohfeld sought to categorise 'rights' into clear and unambiguous parts. Thus, an entitlement might be proper or claimed. An entitlement might also be a legitimate entitlement (e.g., an entitlement under which an individual could be required to undertake or refrain from undertaking an action) representing an equivalent duty in a person.

Under Hohfeld's views about property rights, there is no unified concept describing private property as a natural right or an intellectual creation under the law. On the contrary, the law grants rights over tangible objects to particular individuals.[33] Further, any property that an individual holds is simply the sum total of a set of specific rights that the law has granted to him or her in that state. Such rights have been metaphorically referred to as 'sticks' and the property that an individual holds is the particular bundle of 'sticks' the law grants to them in a given situation. Thus, the law can reform the subject matter of property rights by adding or removing 'sticks' from a bundle.

Hohfeld also argued that, under the law, rights can be broken down into constituent element blocks upon which more complex legal rights can be

30 Wesley Newcomb Hohfeld, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) *The Yale Law Journal* <http://archive.org/details/jstor-785533>.

31 Henry E. Smith, 'Property is not just a Bundle of Rights' (2011) 8 *Econ Journal Watch* 279.

32 Thomas W. Merrill and Henry E. Smith, 'Making Coasean Property More Coasean' (SSRN Scholarly Paper ID 1758846, 9 February 2011) *Social Science Research Network,* <http://papers.ssrn.com/abstract=1758846>.

33 A Kameas et al, 'An Architecture that Treats Everyday Objects as Communicating Tangible Components', *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications,* 2003. (PerCom 2003) (2003) 115; Richard A Epstein, 'Liberty versus Property? Cracks in the Foundations of Copyright Law' (SSRN Scholarly Paper ID 529943, 1 April 2004) *Social Science Research Network* <http://papers.ssrn.com/abstract=529943>; Michael J Madison, 'Law as Design: Objects, Concepts and Digital Things' (SSRN Scholarly Paper ID 709121, 27 April 2005) *Social Science Research Network* <http://papers.ssrn.com/abstract=709121>.

built. Hohfeld termed these basic rights as 'jural relations' (i.e. legal relations) of which the following two are of paramount important in terms of the conceptualisation of property: power and immunity. Hohfeld's analysis showed that property was not as simple a notion as it first appeared; rather, property comprises a particular pack of determinate types of Hohfeldian legal relations.[34] In accordance with Hohfeld's logic, property can be conceptually analysed in relation to particular rights that the law gives to the Aristotelian individual. A subliminal link exists between Aristotle and Hohfeld's notions on the importance of individuals. Further, this link highlights the importance of personal growth and the further social benefits to Plato's republic or state. Since the first introduction of the concept of property, philosophers have considered personal growth continuously. Despite its long history, property as a concept and the subject of philosophical considerations has only recently been the subject of discussion within different disciplines (i.e., disciplines other than the law) and it is through these discussions that the complexity of the content has become clear.[35] This provides additional justification for Hohfeld's view that the concept of property is built on complex rights and legal relations.[36]

This theory does not provide a new normative notion; rather, it provides analytical and descriptive notions (despite its origins within a long-lasting and critical philosophical debate on legal rights and legal liberties).[37] Hohfeld's views approach Plato's in relation to joint ownership. In particular, under Hohfeld's theory and from a legal perspective, the concept of property is complex, contains no element or connection with the narrower concept of private property. Thus, by showing that there is no determination of private ownership and detailing the limits private ownership, joint ownership emerges as a necessity. The origins of property as a concept that

34 Curtis Nyquist, 'Teaching Wesley Hohfeld's Theory of Legal Relations' (2002) 52 *Journal of Legal Education* 238.

35 Peter K. Yu, 'International Enclosure, the Regime Complex, and Intellectual Property Schizophrenia' (SSRN Scholarly Paper ID 1007054, 15 August 2007) *Social Science Research Network* <http://papers.ssrn.com/abstract=1007054>.

36 May, above n 24.

37 Denise R Johnson, 'Reflections on the Bundle of Rights' (2007) 32 *Vermont Law Review* 247; Hugh Breakey, 'Property Concepts' [2012] *Internet Encyclopedia of Philosophy* <http://www.iep.utm.edu/prop-con/>.

lies in Plato's philosophy in relation to the communal use of property represents a more desirable model that can be used to justify the philosophy of open access.

3.4 Justifications for the extension of property to intellectual Creations

Intellectual property refers to original expressions of thoughts and new applications of ideas.[38] The quantity of intellectual efforts and its related market have developed considerably over the course of the last century due to creations stemming from ongoing technological advancements.[39] Consequently, under this technological progress, another aspect of property that must be considered is tangible profits, as intellectual creations are affiliated with such profits.[40]

Robert Merges, a notable scholar in the area of intellectual property theories, claims that property does have a future. He states that if property has proper respect in the context of interplay between owners and social needs, it could contribute beneficially to a well-organised socio-political regime.[41] However, as long as modern society's profitable resources are intangible will be served by the crucial part of property law referred to as intellectual property.[42] Merges outlined the basic features for a workable justification

38 Mark A Lemley, 'Property, Intellectual Property, and Free Riding' (2004) 83 *Texas Law Review* 1031.

39 Nagesh Kumar, 'Intellectual Property Rights, Technology and Economic Development: Experiences of Asian Countries' (2003) 38 *Economic and Political Weekly* 209; Lei Yang and Keith E Maskus, 'Intellectual Property Rights, Technology Transfer and Exports in Developing Countries' (2009) 90 *Journal of Development Economics* 231.

40 Cyril Ritter, 'Refusal to Deal and Essential Facilities: Does Intellectual Property Require Special Deference Compared to Tangible Property?' (SSRN Scholarly Paper ID 726683, 26 May 2005) *Social Science Research Network* <http://papers.ssrn.com/abstract=726683>; Emanuela Arezzo, 'Struggling around the Natural Divide: The Protection of Tangible and Intangible Indigenous Property' (2007) 25 *Cardozo Arts and Entertainment Law Journal* 367.

41 Robert P. Merges, *Justifying Intellectual Property* (Harvard University Press, 2011). See also Richard Spinello & Maria Bottis, *A Defense of Intellectual Property Rights*, Edwad Elgar Publishing, 2009.

42 Ikechi Mgbeoji, '*Justifying Intellectual Property*' (2012) 50 Osgoode Hall Law Journal 291.

of intellectual property as follows: a) the properties of creative labour (as a form of creative work) should be recognised and rewarded with true legitimate rights; thus, work from hourly wages should be converted into a freestanding economic asset whenever possible b) granted and real rights, but not absolute rights, acknowledge creator's and society's contribution to the creative work and c) the accommodation of end-users' needs by facilitating and encouraging cost-effective and convenient intellectual property permission and licencing tools and methods that allow a binding dedication of the rights to the public. This last element of intellectual property provides additional support to the argument of this paper with regard to the desirability of open access model.

Currently, the economic perspectives of intellectual property outweigh other perspectives and thus help us to understand that these perspectives should be considered. Thus, economic justifications for intellectual property should be addressed as they are additional factors that determine whether the concept of property should be extended to creative endeavours. Further, economists have explored ways to efficiently allocate scarce resources to unlimited wants and have noted that intellectual property rights are a plausible way of dealing with the issue of scarcity in an efficient manner.[43]

Another significant justification is that of utilitarianism. Proponents argue that technological inventions are utilitarian works; thus, utilitarianism has been the principal economic theory applied. Utilitarian theorists generally endorse the creation of intellectual property rights as an appropriate instrument to foster innovation.[44] It is acknowledged that freedom of expression and the creation, dissemination and protection of information ought to co-exist to support effective outcomes (e.g. innovation). However, this justification illustrates the importance of creators' rights and efforts

43 Meir Perez Pugatch, *The International Political Economy of Intellectual Property Rights* (Edward Elgar Publishing, 2004); Meir Perez Pugatch, *The Intellectual Property Debate: Perspectives from Law, Economics and Political Economy* (Edward Elgar Publishing, 2006).

44 Peter S Menell, 'Intellectual Property and the Property Rights Movement' (SSRN Scholarly Paper ID 1000061, 12 July 2007) *Social Science Research Network* <http://papers.ssrn.com/abstract=1000061>; Peter S Menell, 'The Property Rights Movement's Embrace of Intellectual Property: True Love or Doomed Relationship?' (SSRN Scholarly Paper ID 965083, 1 February 2007) *Social Science Research Network* <http://papers.ssrn.com/abstract=965083>.

and distinguishes social evolution. Thus, information needs to be both protected and shared.[45]

The majority of authors who have adopted economic analyses of intellectual property have relied on the 'Kaldor-Hicks' criterion that counsels lawmakers to select a system of regulations that maximises aggregate welfare measured by end users' ability and willingness to pay for goods and services in relation to information. Thus, three different economic theories dominate the literature. First, the most common, incentive theory claims that the optimal doctrine maximises the difference between (a) the current discounted value to the end users of intellectual products (created because the inventors were induced by the possibility of a monopoly power) and (b) the ensemble detriments generated by a system of incentives. In uneven terms, this theory urges governmental lawmakers to establish or develop intellectual property protection, as doing so will assist end users by stimulating their creative efforts more than it would harm them by constricting their access to intellectual property products or raising taxes. The second economic theory is based on patent regimes that reduce rental dissemination. This theory seeks to eliminate or reduce the tendency of intellectual property rights to advance duplicative or uncoordinated inventive activity. Economic waste can occur at three stages in the inventive process.

Copyright and patent systems play the crucial role of letting potential producers of intellectual products know what end users want. With this information, these producers can channel productive outcomes in the direction most likely to enhance end users' welfare. Based on this rationale, sales and licenses will ensure that goods are delivered to people who need them and are able to pay for them. Only in specific circumstances (i.e. when transaction costs prevent such voluntary exchanges) should the holders of intellectual property rights be denied total scrutiny in relation to the use of their works.

45 Réjean Landry, Nabil Amara and Moktar Lamari, 'Does Social Capital Determine Innovation? To What Extent?' (2002) 69 *Technological Forecasting and Social Change* 681; David Lane et al, *Complexity Perspectives in Innovation and Social Change* (Springer Science and Business Media, 2009); Stephen J. Guastello, *Chaos, Catastrophe, and Human Affairs: Applications of Nonlinear Dynamics to Work, Organizations, and Social Evolution* (Psychology Press, 2013).

4. Open access as additional support for the modern copyright protection in the digital age

Scholars have been communicating and examining thoughts, considerations, claims and research outcomes throughout the ages within a variety of forms. Lectures, discussions, essays, manuscripts, monographs, articles and books are common ways that intellectual ideas or scholarship have been shared. With the coming of the Enlightenment age, the first scholarly periodicals (i.e., *Philosophical Transactions of the Royal Society of London* and the *Journal des scavans*) were published in 1665 by leading learned societies.[46]

Since then, scholarly articles have become the principal form for effective scholarly communication.[47] Learned societies managed the editing and publishing of scholarly journals during these early times.[48] Today, the approach remains the same as scholarly societies continue to publish some of the leading journals on a variety of scientific areas. After World War II, government investments in Western Europe and the United States (US) in the field of scientific research increased the class of researchers communicating with their fellow scholars. However, at the same time, the learned societies were slow to adapt to this instant flow of information and representatives of the printing press industry entered the area in growing numbers to provide new titles in a variety of scientific areas.

The growing number of publications obliged subscribers of scholarly journals, including academic libraries, government agencies and industrial research to obtain access to scholarly data.[49] The expenses affiliated with such access began to increase with the rise of electronic publications.[50] Fur-

46 David J. Weber, *Barbaros: Spaniards and Their Savages in the Age of Enlightenment* (Yale University Press, 2005).

47 Carl Bergstrom, 'Measuring the Value and Prestige of Scholarly Journals' (2007) 68, 314; Carol Tenopir et al, 'Electronic Journals and Changes in Scholarly Article Seeking and Reading Patterns' (2009) 61 *Aslib Proceedings* 5.

48 James Hopkins, 'The Role of Learned Societies in Knowledge Exchange and Dissemination: The Case of the Regional Studies Association, 1965–2005' (2011) 40 *History of Education* 255.

49 Danah Boyd and Kate Crawford, 'Critical Questions for Big Data' (2012) 15 *Information, Communication and Society* 662.

50 Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth*

ther, journal publishers were forced to produce their content in two different forms (i.e., hard copy journals and electronic/digital versions, hosted on a digital network). The costs of scholarly journals increased, as did concerns about how affordable access to these journals could be maintained. Further, the development of Internet created a number of new terms, challenges and circumstances in respect of scholarly communication. Thus, the printing press started shifting its operations to keep up with the digital platform of Internet, which was attracted by cost effective solutions.

The Internet revolutionised computers and communicating. The invention of the telegraph, telephones, radios and computers set the stage for this unprecedented integration of capabilities. The Internet has a world-wide broadcasting capability, a mechanism for information distribution and is also a medium for collaboration and interaction between individuals and their computers regardless of geographic locations. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and the development of an information infrastructure. Beginning with early research on packet switching, the government, industries and academics have worked together to evolve and deploy this exciting, new technology. The Internet emergence created the possibility of extending access to the scholarly articles in cost-effective ways and in circumstances where the scholarly printing press had become dominated by for-profit publishers (rather than non-profit scholarly societies) and increasingly consolidated. By using their collective pricing power, publishers set journal subscription prices and obliged academic libraries and other subscribers to pay these prices to have the benefit of accessing up-to-date research.

A renowned author in the field of open access, Michael Carroll, argues that the concept of open access was born out of the frustrations caused by the increasing diffusion of scholarly research through Internet and the ever-rising price of journal subscriptions.[51] These frustrations led academ-

Network, and the Rise of Digital Utopianism (University of Chicago Press, 2010); David Lyon, *The Electronic Eye: The Rise of Surveillance Society—Computers and Social Control in Context* (John Wiley and Sons, 2013).

51 Michael W. Carroll, 'The Movement for Open Access on Law' (2006) 10 *Lewis and Clark Law Review* 741.

ic librarians, autodidacts and other academic leaders to unite and initiate open access. Carroll argues that the principal objective of open access is to enable further access to scholarly literature and relevant information resources and ensure that these materials are freely within Internet for end-users and researchers.[52]

Open access reduces the obstacles to the online availability of information that end users should enjoy by using scholarly journal articles. However, copyright protection issues emerge and should be considered. In this context, advocates argue that there are two ways within which scholars can make their articles accessible and copyright protected; either by publishing *via* the 'gold road' of open access through which publications are freely available online or by publishing *via* the 'green road' of open access in subscription-access journals in which authors self-archive an e-print of their work in an online open access repository[53] Once an article is freely accessible within either method, it is indexed by search engines, immediately locatable and retrievable by anyone with internet access.[54] Taking everything into account, the concept of open access is a response to current technological developments in conjunction with creative efforts that should be formulated and attached to modern copyright laws, appropriately.

5. Conclusions

A clear issue in the various theories of property ownership relates to the proper equilibrium between self-interest and the social good. Property philosophers engage in devising appropriate means to balance individuals' interests with the common good. From my point of view, conceptualization of property should consider, amongst others, Plato's views for justice, Aristotle's ideas for private ownership, Locke's theories of labour, Hegel's notions of personality growth and Hohfeld's full account of ownership rights.

52 Michael W. Carroll, 'Creative Commons and the Openness of Open Access' (2013) 368 *New England Journal of Medicine* 789.

53 Stevan Harnad, 'The Green Road to Open Access: A Leveraged Transition' <http://users.ecs.soton.ac.uk/harnad/Hypermail/Amsci/3379.html>.

54 Stephen Cramond, 'Explainer: Open Access vs Traditional Academic Journal Publishers' (July 27, 2011) *The Conversation* <http://theconversation.com/explainer-open-access-vs-traditional-academic-journal-publishers-2511>.

The main feature of the above theories is that the concept of property led to the evolution, production and intellectual creativity. Subsequent philosophers elaborated on this notion, but, being influenced by their specific social surroundings, attributed different traits to the concept of property.

How did the concept of property ownership inform the development of notions of intellectual property and relevant endeavors? Intellectual property refers to rights associated with the expression of an idea or some other abstract object.[55] Thus, intellectual property refers to the 'goods' created by human minds. Forms of intellectual property include patents, trademarks and copyrights. The notion of intellectual property rights was originally created to protect the creative procedures of inventors and scientists and benefit society as a whole. However, by increasing this 'shield' of protection, an inverse result occurred. Consequently, a number of alternative initiatives were implemented in the early nineties to protect intellectual property that, in response to the progressively high level of capitalisation of intellectual property rights, placed less emphasis on the trade element.

55 Adam Moore and Ken Himma, 'Intellectual Property' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (2014) <http://plato.stanford.edu/archives/win2014/entries/intellectual-property/>.

Understanding Digital Piracy through the Lens of Psychological, Criminological and Cultural Factors

by Sanjeev P. Sahni[1], Garima Jain[2] & Indranath Gupta[3]

1. Introduction

Producers of digital products all over the world are actively fighting the spread of pirated copies of their product. It has been generally argued that piracy generates unemployment, encourages tax evasion, infringes intellectual property, provokes unfair competition in economy, generates inflation and stimulates organized crime (Karaganis, 2011).

Experts from varied discipline ranging from psychology, sociology, political science, and economics have examined the rationale behind digital piracy (Sundararajan, 2004; Higgins et al., 2006; Gopal et al., 2004; Morris and Higgins2010; Bagchi et al, 2006). Zhang (et al.,2009) propounded that digital piracy feels more acceptable to people than physical theft. Criminologists and legislators study digital piracy differently from street crime or physical crime (Morris and Higgins, 2010). In comparison to physical form of piracy, often, online piracy lacks negative social stigma. At times, individuals are not conscious that they are involved in infringing activity by purchasing pirated software, books, movies or music. Public awareness about intellectual property laws at large represents a significant explanation of software piracy rates (Hsu and Shiue, 2008).

There are number of measures adopted by legislatures, economists and governmental organizations to curb digital piracy. The role of psychologi-

1 Principal Director and Professor of Jindal Institute of Behavioural Sciences, O.P. Jindal Global University (JGU), email: drspsahni@jgu.edu.in.

2 Sr. Research Associate at Jindal Institute of Behavioural Sciences and Assistant Director at Center for Victimology and Psychological Studies, O.P. Jindal Global University, email: gjain@jgu.edu.in. Corresponding Author.

3 Associate Professor and Assistant Director, Centre for Post Graduate Legal Studies & Assistant Director, Centre for Intellectual Property and Technology Law, Jindal Global Law School, O.P. Jindal Global University, email: igupta@jgu.edu.in.

cal, sociological and cultural factors in the context of digital piracy has seldom been discussed in developing nations, although considerable amount of research is done in developed nations.

This paper aims to critically review the research concerning psychological, sociological and cultural factors affecting behaviour towards digital piracy in the last two decades. It will identify potential area of future research based on critical construct of existingliterature.

As a part of the paper, a total of 624 studies were identified, which discussed the phenomenon of digital piracy, its prevalence and various factors ranging from economic, political, legal, cultural, psychological, behavioural, criminological and sociological factors leading to downloading and uploading of unauthorized content. Out of 624, 98 studies were further shortlisted by following an inclusion criteria of psychological, sociological and cultural factors that impact the behaviour of the perpetrators of digitalpiracy.

The chapter concludes on a note that the phenomenon of digital piracy can be understood through the lens of multiple factors other than using the framework of legal and economic factors. While it has been claimed that digital piracy is more prevalent in emerging economies, there is a need for a cross-country research involving emerging and developed economies to study the importance of psychosocial and cultural factors influencing digital piracy.

2. Background

The Internet and the development in digital technology have brought about dramatic improvements in the quality of life for many individuals in the world, although this confluence has also provided the haven for discrepancy and crime (Adler and Adler, 2006).

Digital piracy is an act of illegitimate duplication of digital media, which may include the act of sharing files or illegally downloading using peer-to-peer file sharing network (Gopal et al., 2004). With the increase in commercialization of internet, there has been increase in digital piracy in recent years. Access to internet has enabled individuals to easily commit criminal activity for four reasons: it allows anonymous communication, it is transnational, there is a shift in the idea of ownership of physical prop-

erty to the ownership of ideas, and it is relatively easy (Wall, 2010). Further on, internet facilitates piracy because the structure of the internet allows the offense to take place away from the copyright holder, leaving the perception that the act is victimless.

While media piracy has become a 'global menace', 'international plaque' and 'ubiquitous', it is further interesting to see the trend in emerging economies (Banerjee et al. 2005). It has been established that digital piracy is more prevalent in emerging economies than developed economies (Karaganis, 2011). According to BSA (2013) report, emerging economies accounts for 56% majority of all PCs in use globally and it comprises of 73% of all unlicensed software installation. It is estimated that this trend is likely to continue as it is found that 65% of OC software downloaded in emerging economies are properly licensed as compared to 23% in developed economies. Asia Pacific is found to be the region with highest rate of illegitimate PC software installation- China (74%) and India (60%).

3. Digital piracy: psychosocial, criminological and cultural factors

Digital Piracy has become a salient topic in legal, economic and political milieu (Hinduja and Ingram, 2009). World's leading reports on piracy published by World Intellectual Property Organization (WIPO), BSA, have not explicitly explained the act of digital piracy from a behavioural, psychosocial, cultural and criminological perspective. There is, however, enough indication to suggest that infringement of intellectual property is as significant as robbery and burglary (Luckenbill and Miller, 1998). It is important to study the psychosocial and cultural factors leading to the act of digital piracy to reduce it in the cyberspace. In a cross-country analysis of music piracy involving 26 countries by Walls, in 2008, it has been suggested that piracy increases with the issue of collectivism and social coordination within society, whereas the rate of income has insignificant impact on the level of piracy in any nation. It has been found by Sheehan, Tsao and Yang (2010) that economic, social and collective utilities motivate the gratification of digital music piracy among college students, with social utility being the most important factor. These studies reinforce the need to study the phenomenon of digital piracy from a psychological, cultural and sociological perspective.

3.1 Social learning theory and digital piracy

While postulating the social learning theory, Akers (2011) suggested that criminal behaviour is learned through association with people. He also proposed the sequence of such learning and its manifestation. Once a social environment is created consisting of associations of people inclined to criminality, patterns of imitation are likely to be followed. With further reinforcing stimuli, the deviant behaviour may be perpetuated. Akers (1992) and Akers and Lee (1996) further stated that the relationship between individual and social processes is influenced by a person's models of behaviour, conducive or aversive environment to crime commission, and differential reinforcement.

Gottfredson (1987) cited the connection between deviant peer association and deviant behaviour and stated that "people acquire the propensity to delinquency, find delinquent friends and then, commit delinquent acts, including serious criminal acts". There are numerous scholarly and research articles, which presented social learning theory as an appropriate framework to understand deviant online behaviour (Higgins and Wilson, 2006; Higgins et al, 2007; Hinduja and Ingram, 2009; Higgins and Makin, 2004; Skinner and Fream, 1997). In a survey involving 2000 university students by Hinduja and Ingram, (2009), it has been suggested that both online media sources (chat rooms) and peer influences are significant to predict music piracy. This study further expressed that the behaviour of piracy can be explained by offline (friends, acquaintances, group discussion) and online communication (email, chat rooms, instant messaging programme). In fact, participants who associate with those who display a tolerance towards deviance and illegal downloading had higher piracy scores. In the context of music piracy, it has been suggested that pervasive online theft of intellectual property can be curbed by encouraging ethics pertaining to the practice of information technology and acceptable rules of engagement (Higgins and Wilson, 2006). This study, however, was limited to student population, thereby restricting the generalizability of findings to other population. The findings were based on self-reported assessment of participants with the possibility of under-reported cases of music piracy.

Individuals living in a conducive environment towards piracy are more likely to indulge in the act of digital piracy (Higgins and Wilson, 2006; Higgins and Makin, 2004; Higgins et al, 2007; George, 2009). Hence, Higgins

and Wilson, 2006 recognized social environment to influence the attitude and behaviour of individuals. An empirical study conducted by Higgins, Marcum, Freiburger and Ricketts, 2012 involving 287 students in the United States suggested that peer association has significant connection with digital piracy.

To address the issue of digital piracy, there is a need to modify social attitude, belief and behaviour towards intellectual property protection and marketing strategy of software developers. Effective law enforcement alone will not address the issue (Lau, 2003). It was further revealed that although people are aware that piracy is illegal, they are prepared to do it, if the behaviour is socially acceptable. People change their perception, attitude and consequently behaviour as per existing value system of society in general (Baron, 1984). If the perception is inconsistent with societal norms and values, there is a greater tendency for people to change their own value system (Givon, 1995).

There had been studies looking into behaviour that supports the willingness to pay for a non-pirated software and the factors that affect such behaviour. One of such studies led by Hsu and Shiue (20080 administered a consumer survey to a sample group of 799 students from various schools and colleges in Taiwan. It was observed from the study that while the social norms positively influenced the willingness to pay, however the prosecution risk did not have much of an effect on the intention to own pirated software. The study did not look into the cross-culture variation and its effect on the willingness to pay for original software.

The minor significance of legal sanctions was again highlighted in a separate research wherein 34 persistent pirates were interviewed by Holt and Copes (2010) to study justifications, practices, risk and rewards associated with digital piracy. The findings suggested that pirates share a belief which structures their identity and develops relationship with other pirates. The belief further reinforces the perpetrators to commit piracy.

Social and cultural norms also influence digital piracy rate in a society. Piracy has been observed as a group activity as it involves distribution of computer software, songs, videos and movies amongst friends, co-workers, and relatives (Gopal and Sanders, 1998). Essentially, individualism and collectivism are two accepted cultural dimensions of a society (Hofstede et al., 2010). Husted demonstrated that cultural variables such as power

distance, individualism, masculinity and uncertain avoidance (the extent to which members of a culture feel threatened by uncertain and unknown situations) determine the rate of software piracy in a region (Husted, 2000).

In collectivistic societies, group influence exert a pressure on individuals to share their resources. As a result, individualistic societies tend to involve lesser in digital piracy (Husted, 2000; Marron and Steel, 2000; Shinet al., 2004). Notwithstanding this trend, emerging individualistic countries like South Africa and Mexico have overwhelming piracy rates.

The effect of collectivistic society and individualistic society was again observed by Chiou et al., 2011 in a study involving 219 college students of Taiwan and 252 students of the United States. The research observed the effects of perceived risk of getting caught other than looking into cultural dimension of attitude and intention towards music piracy. Perceived risk of getting caught can significantly reduce the act of music piracy in both countries. The study further advocated that stringent legal sanctions can curb piracy significantly in Taiwan than the country in comparison. The United States falls under the category of an Individualistic Society and Taiwan has been considered as a collectivistic society (Triandis, 1994). It was found that collectivistic culture acts as a motivator for downloading illegal music files. Further, there were suggestions to include more countries to understand the impact of different cultures (collectivistic and individualistic) and environmental factors on digital piracy. It has been already indicated by Walls (2008) in the cross-country analysis of 26 diverse nations that piracy increases with increase in the level of collectivism and social coordination.

3.2 Self-control and the act of digital piracy

Linking self-control as a predictor in explaining criminal behaviour has been established by Gottfredson and Hirschi, 1990; Gottfredson, 1987. The act of digital piracy does amount to deviant or criminal behaviour (Zhang et al., 2009; Wall, 2010). Researchers have demonstrated relationship between self-control and digital piracy (Higgins, 2004; Higgins and Wilson, 2006; Higgins and Makin 2004; Higgins et al., 2008). Krueger et al. (1996) established that individuals with low self-control are more likely to project instant gratification and, as a result are less likely to wait for the original

version of digital media. They will be more attracted towards thrill, ease and immediate acquisition of the digital software or music file and will be less sensitive towards copyright agreement associated with a digital media. Using multiple parameters like personality measure (Grasmick et al., 1993) social bonding (Hirschi and Gottfredson, 1994) and inhibition measure (Piquero, 2007; Higgin et al., 2008), it has been suggested that individuals with low self-control are more likely to be involved in digital piracy. Individuals with high regards for family members, parents and school (high social bonding) are less likely to get involved. Further, individuals with greater self-generated inhibitions are less likely to become the perpetrators, while individuals with low self-control are more likely to involve in deviant online behaviour (Higgins et al., 2007).

A self-reported questionnaire filled by 337 respondents in the United States studied socio-demographic variables alongside previous pirating behaviour, low self-control and ethical predisposition in explaining deviant peer association. With age, individuals are less likely to associate with deviant peers. This study further elucidated that low self-control not only predicts high pirating behaviour, but it is a factor that leads to association with deviant piracy peers (Wolfe and Higgins, 2009).

It has been contended by previous researchers that there exist a theoretical (Akers and Cochran, 1985; Akers, 2011; Evans et al., 1997; Gottfredson and Hirschi, 1987; 1990) and empirical (Gibson and Wright, 2001; Higgins and Makin, 2004; Longshore et al., 2004; Wrightet et al., 1998) link between self-control and social learning theory. Further a study involving 332 university undergraduates developed a three-factors model showing the relationship between self-control, social learning theory and digital piracy. This study suggested that social learning has a mediating effect on low self-control and digital piracy. Individuals with low self-control and association with deviant peers are more likely to be involved in digital piracy. Further suggestions have been made to study theoretical constructs of self-control with other variables or theories, which may have substantial significance on understanding digital piracy (Higgins et al., 2007).

3.3 Neutralizing techniques and justifications of perpetrators

Zhang et al. (2009) unveiled that digital piracy feels more acceptable to people than physical theft. Psychologists at the University of Notre Dame,

Crowell et al. (2005) furthered that economic factors may provide pirates with a means to justify their actions, but they are not the real motivators. Computer appears to act like an ethical filter. It creates a "psychological distance between creator and pirate." Easy accessibility, autonomous and anonymous identity and asynchronous nature of communication have contributed to highly psychoactive experiences in the online world. Moreover, chances of detection, apprehension and prosecution over internet are exponentially smaller (Hinduja and Ingram, 2009).

A study of 2.032 undergraduates from Midwestern University by Ingram and Hinduja, 2008 revealed the extent of neutralization techniques in anticipating the participant's involvement in music piracy. There are five types of justification: denial of responsibility ("it is not my fault"), denial of injury ("no harm will result from my actions"), denial of victim ("nobody got hurt"), condemnation of the condemners ("how dare they judge me, considering how corrupt and hypocritical they themselves are"), and appeal to higher loyalties ("there is a greater and higher cause") (Sykes and Matza, 1957; Skyes and Matza, 2003).

Digital piracy is considered as a white collar crime (Gopal et al., 2004) and researchers postulate that neutralization technique is more prevalent among organizational and white collar crime (Maruna and Copes, 2005). Individuals are more likely to justify or excuse their behaviour when they are partially committed to the deviant activity (Maruna and Copes, 2005). Ingram and Hinduja (2008) further analyzed that neutralization is a significant framework in understanding music and movie piracy. In fact, 90% of the college participants in a study believed that downloading of illegal music files is an appropriate behaviour owing to a myriad of neutralization and justifications to the deviant behaviour (Ingram and Hinduja, 2008). In a study involving thirty four persistent pirates by Halt and Copes (2010) found denial of responsibility as a common neutralizing technique acting towards a justification to their deviant behaviour. Further in a different study, computer science students admitted their involvement in software piracy and it was found that in spite of acknowledging the immoral character of their actions, they were indifferent to the cost borne by software developers (Konstantakis et al., 2010). Using a semi-structured interview technique, the research found that high cost of genuine software, conducive academic environment for piracy and student status is a major excuse, rationale or justification behind students' involvement in the acts of digital piracy.

3.4 Ethical, moral and religious disposition and digital piracy

The moral judgment of individuals towards digital piracy can be understood by Kohlberg's level of moral development. Kohlberg developed three stages of moral development with two sub-stages in each stage.

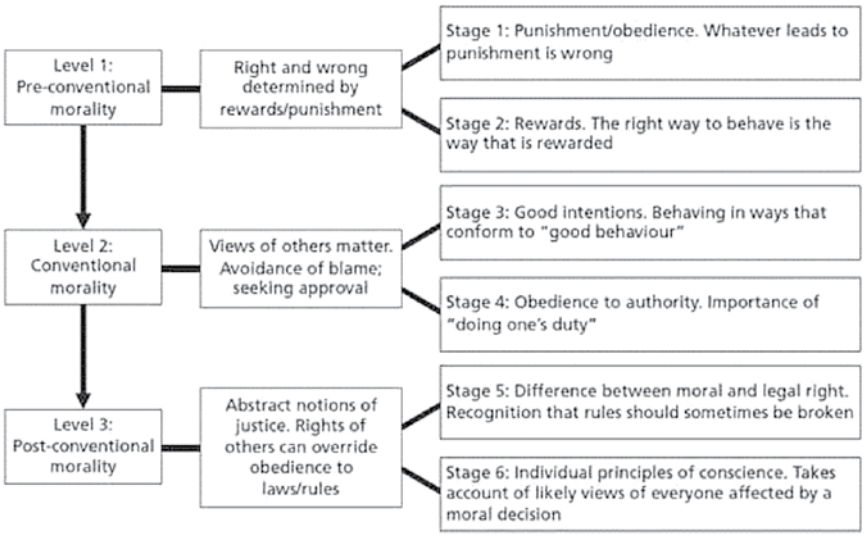


Figure 1: Stages of moral development4

The idea behind this theory is that as individuals grow intellectually, they also grow morally (Gould, 2011). In a study involving business school students, it was suggested that shoplifting was considered to remain in the 1st stage of the second level of Kohlberg's table where peer pressure defined influence. Connecting the act of copying of software to shoplifting, the report concluded that the moral consequence of copying software is less significant for users than the act of shoplifting (Egan and Taylor, 2010). The majority of research and scholarly articles have shown that students are most likely to indulge in the act of digital piracy and hence, most of the research on digital piracy has concentrated on students as their target sample of study. A cross-country comparative research administered by Kini et al.

4 Kohlberg, L, "Stages of moral development" (1971), *Moral Education*, pp.23-92.

(2003) involving 843 students in the United States and 663 students from Thailand showed the difference in the perceived moral intensity towards software piracy. It has been found that students in the United States have higher mean scores of moral intensity than students from Thailand. However, the factors which define higher moral intensity in the United States have not been stated and defined in the study.

It has been established that individuals with lower ethical predispositions are more likely to get involved in digital piracy (Hinduja and Ingram, 2004; Hinduja and Makin, 2004; Higgins and Wilson, 2006). Students do not take into consideration moral values and predisposition, while downloading unauthorized software from internet (Siegfried 2001). The act reflects that individual interest outweighs the presence of moral issue (Konstantakis et al. 2010). Further, moral predisposition of a student towards the act of digital piracy also depends on how others, including fellow students, professors and administrative staff contemplate the issue[5].

Researchers have confirmed that students consider piracy as a low moral issue and give economic reasons as justification behind their involvement in the act (Lau, 2003; Al- Rafee and Cronan, 2006; Cronan and Al Rafee, 2008).

In the course of developing a Behavioural Model of Digital Piracy, a questionnaire was administered to 133 students who were at an undergraduate level of business studies (Gopal et al., 2004). This study was based on a deontological theory of ethical behaviour, which states that a person's intentions are based on his ability to evaluate goodness of his actions, which is further influenced by the principle of utility. This utility principle states that many perceive an action to be right, if it causes the greatest good for the most number of people possible. The results of the study indicated that age of the actor, value of the product, popularity and lack of awareness are some of the factors that influenced musicpiracy.

While most of the studies concentrated on understanding digital piracy in developed countries, one out of the very few studies concentrated on Arab and Middle Eastern Country to reflect upon the effect of religion, law and awareness on digital piracy. Al Rafee and Rouibah (2003) analyzed that out of a total sample size of 319 students, it was observed that religious

5 Supra, note 58.

and aware group showed a significantly less intention to engage in piracy. However, such intention varied with age groups and different sections of the society. Additionally, the study was conducted in a conservative Islamic Country, which may have been the reason for religious factors having a major impact on the overall results. This situation could be different in countries practicing other religions or in less conservative societies. The study did not take into consideration all these factors. Therefore, the findings of this study cannot be generalized to everyone around the globe.

A study conducted in 2014 (Kos Koklic et al., 2014) looked into the role of perceived risk and moral risk on the attitude and behavioural intentions of adult computer users. It established a significant impact of perceived moral intensity and perceived consequence of digital piracy on society and consumer's overall attitude towards digital piracy.

3.5 Theoretical constructs in explaining digital piracy

Researchers and academics all over the world have tried to investigate digital piracy phenomenon through various behavioural theoretical constructs like the Theory of Reasoned Action (TRA) (Fishbein and Aizen, 1975) and the Theory of Planned Behaviour (TPB) (Aizen, 1991).

Since late 1980s and early 1990s, a number of efforts have been made to study digital piracy. The TRA constructed by Fishbein and Ajzen (1975) is regarded as most fundamental and significant theory to explain human behaviour. Christian and Eining (1991) employed TRA model and studied the factors influencing software piracy. A study of 139 undergraduate accounting students indicated that attitude, material consequences and normative expectations are significant factors that explain behaviour relating to piracy. Loch & Conger (1996) conducted an exploratory study and used TRA to describe ethical decision in making the use of computer. The study revealed that self-image, deindividuation and computer literacy had a significant impact on attitude and intention to computer privacy and ownership. They, however, concluded on a note that TRA does not adequately encapsulate ethical decision making process.

To test the theory of planned behaviour, expected utility theory and deterrence theory, a study involving 201 respondents was conducted to understand software piracy (Peace et al., 2003). The research further drew

attention to the fact that punishment severity and the cost of software and punishment certainty had a connection with software piracy. To further study the above theories and to validate the generalizability of the model in cross-cultural scenarios and different segments of society, a study was conducted by Yoon, 2011 on 270 undergraduate students in China proposed for an integrated model-TPB and ethics theory to study digital piracy. It has been suggested that moral obligation and the justice component of Ethics Theory and TBP variables like subjective norms, attitude and behavioural control, influence the intention to commit piracy.

A pilot study involving twenty students from two universities in Europe investigated the intention to share media files over peer-to-peer networks (Blake and Kyper, 2013). They contended that the theory of planned behaviour can explain significant differences in the intention to share media files (both legitimate and pirated files) over P2P network. It has been recommended that a comparative study of China and Europe must be conducted to investigate cross-cultural variation in measuring file-sharing and predicting actualusage.

Taylor et al. (2009) observed the social psychological foundations underlying the behaviours related to digital piracy. Adopting Perugini and Bagozzi's model of Goal Directed Behaviour, the influence of motivation, frequency of piracy and perceived control on the intention to indulge in movie and music piracy was assessed by Blake and Kyper, 2013. Participants were divided in to two groups including those who were intended to engage in music or movie piracy and those who would like to refrain from indulging in music or movie piracy. The model anticipated 20% to 68% variance in intention of the participants depending on their representation in their respective groups.

The application of Social Cognitive Theory (SCT) was also extended to downloading behaviour of pirates (LaRose and Kim, 2006). College students from Midwestern University were studied in this research. SCT was considered most appropriate to study deviant behaviour like downloading as it includes (coping) self-efficacy and (coping) self- regulation. Coping self-efficacy relates to an individual's perceived ability to handle negative events, whereas self-regulation includes self-control. The behaviour of habitual file sharing and downloading hundreds and thousands of songs without listening to those songs is a projection of poor self-regulation. The

outcome of file sharing was predicted through SCT and was not perceived in the framework of Theory of Planned Behaviour.

3.5 Critical constructs of the review

Broadly speaking, there are certain shortcomings of the existing research explaining the act of digital piracy. This can be summarized into three areas covering the following issues.

3.5.1 Sample demographic of majority research include only students

The majority of research projects, which studied digital piracy have based their exploration on the sample target of either undergraduate or graduate students from one to two universities (Chiou et al., 2011; Christensen and Eining, 1991; Cronan and Al-Rafee, 2008; s'Astous et al, 2005; Wolfe and Higgins, 2009; Gopal et al., 2004; Higgins and Makin, 2004; Higgins et al., 2006; Higgins et al., 2007; Wolfe and Higgins, 2009; Hsu and Shiue, 2008; Husted, 2000; Hinduja and Ingram, 2009; Kini et al., 2003; Lau, 2003; Konstantakis et al., 2010; Siegfried, 2001; Zhang et al., 2009). The studies have demonstrated that students are mostly involved in the act of piracy. Limiting the sample to students, however, restricts the generalizability of findings to other population. To fill the gap, Kos Kokilic et al. (2014), analysed 943 adult computer users and students to study the perceived adverse effects of digital piracy. The study could not draw significant comparative analyses of the perception and attitude of students and adults to digital piracy due to limited sample size. There is a need for future research to study different universities and regional demographics.

Self-report assessment: It has been observed that to analyse the factors associated with digital piracy, authors have administered self-reported assessment method on the respondents (Hinduja, 2006; Wolfe and Higgins, 2009; Lalovic et al., 2012). This method as a tool of assessment is considered both inexpensive as well as efficient by researchers (Robins et al., 2009). They can be easily administered in mass testing sessions and myriad variables can be collected from the respondents in single settings as opposed to one- to- one interview and diary studies. However, responses from self-report method may have been subjected to recall bias, social desirability bias or errors in self- observation. In other words, participants might have underestimated their involvement in the act of digital piracy in order to

adhere to social desirability norm (Hinduja and Ingram, 2009).

Intention and not the actual use: in an effort to measure attitude of digital piracy, most of the studies (e.g. Kwong et al., 2003; Mortan and Koufteros, 2008) focused on measuring intention of the participants and not their actual involvement in the act. Although, intention is a significant factor that determines the actual involvement of individuals in the act, but there might be external or situational factors as well that might influence the decision- making of a user. Intention is not representative of actual engagement in digital piracy. It is imperative to evaluate actual behaviour to develop an adequate model to address the issue.

4. Conclusion

The findings of 68 research studies presented in this paper suggest that predisposition towards digital piracy is influenced by personality factors (self-control), personal or psychological factors (neutralization techniques, attitude and beliefs), social and cultural factors (social learning, collectivistic/individualistic factors). Extensive literature is available on factors other than legal and economic factors, nevertheless, it has been found that these factors are rarely acknowledged by the stakeholders (legislatures, industry, and policy makers) for curbing digital piracy (Bagchi et al., 2006). It is proposed that digital piracy is more prevalent in emerging economies (Karaganis, 2011). This calls for a cross-country research involving emerging and developed economies to study the importance of psychosocial and cultural factors influencing digital piracy, thereby proposing recommendations for the legislatures, industry and policy makers to understand the issue through the lens beyond economic and legal factors.

5. References

1. Adler, P. A. and Adler, P. (2006) 'The deviance society', *Deviant Behavior*, vol. 27, no. 2, pp. 129-148.
2. Akers, R. L. and Cochran, J. K. (1985) 'Adolescent marijuana use: A test of three theories of deviant behavior', *Deviant Behavior*, vol. 6, no. 4, pp. 323-346.
3. Akers, R. L. (1992) 'Linking sociology and its specialties: The case of

criminology', *Social Forces*, vol. 71, no. 1, pp. 1-16.

4. Akers, R. L. and Lee, G. (1996) 'A longitudinal test of social learning theory: Adolescent smoking', *Journal of Drug Issues*, vol. 26, no. 2, pp. 317-343.
5. Akers, R. L. (2011) Social learning and social structure: A general theory of crime and deviance, Transaction Publishers, New Brunswick (U.S.A.) and London (U.K.).
6. Ajzen, I. (1991) 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211.
7. Al-Rafee, S. and Cronan, T.P. (2006) 'Digital piracy: Factors that influence attitude toward behavior.' *Journal of Business Ethics*, vol. 63, no. 3, pp. 237-259.
8. Al-Rafee, S. and Rouibah, K. (2010) 'The fight against digital piracy: An experiment', *Telematics and Informatics*, vol. 27, no. 3, pp. 283-292.
9. Bagchi, K., Kirs, P. and Cerveny, R. (2006) ' Global software piracy: can economic factors alone explain the trend?', *Communications of the ACM*, vol. 49, no. 6, pp. 70-76.
10. Banerjee, D., Khalid, A. M. and Sturm, J. E. (2005) 'Socio-economic development and software piracy. An empirical assessment', *Applied Economics*, vol. 37, no. 18, pp. 2091-2097.
11. Baron, R. A. and Byrne, D. E. (1984) *Social psychology: Understanding human interaction*, Allyn & Bacon.
12. Blake, R.H. and Kyper, E.S. (2013) 'An investigation of the intention to share media files over peer-to- peer networks', *Behaviour & Information Technology*, vol. 32, no. 4, pp. 410-422.
13. Business Software Alliance. (2014) *BSA Global Software Survey*. Retrieved from http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf.
14. Chiou, J. S., Cheng, H. I. and Huang, C. Y. (2011) 'The effects of artist adoration and perceived risk of getting caught on attitude and intention to pirate music in the United States and Taiwan', *Ethics & Behavior*, vol. 21, no. 3, pp. 182-196.
15. Christensen, A.L. and Eining, M.M. (1991) 'Factors influencing software piracy: Implications for accountants', *Journal of Information Sys-*

tems, vol. 5, no. 1, pp. 67-80.

16. Cronan, T.P. and Al-Rafee, S. (2008) 'Factors that influence the intention to pirate software and media.' *Journal of Business Ethics*, vol. 78, no. 4, pp. 527-545.
17. Crowell, C.R., Narvaez, D. and Gomberg, A. (2005) 'Moral psychology and information ethics: Psychological distance and the components of moral behavior in a digital world', in Freeman, L. et al (eds.), *Information ethics: Privacy and intellectual property*, IGI Global, pp. 19-37.
18. d'Astous, A., Colbert, F. and Montpetit, D. (2005) 'Music piracy on the web–how effective are anti-piracy arguments? Evidence from the theory of planned behaviour', *Journal of Consumer Policy*, vol. 28, no. 3, pp. 289-310.
19. Egan, V. and Taylor, D. (2010) 'Shoplifting, unethical consumer behaviour, and personality' *Personality and Individual Differences*, vol. 48, no. 8, pp. 878-883.
20. Evans, T. D., Cullen, F. T., Burton, V. S., Dunaway, R. G. and Benson, M. L. (1997) 'The Social consequences of Self- Control: Testing the General Theory of Crime', *W. Criminology Rev.*, vol. 35, no. 3, pp. 475-504.
21. Fisbein, M. and Ajzen, I. (1975) *Belief, attitude, intention and behavior: an introduction to theory and research*, Massachusetts, Addison-Wiley Publishing Company.
22. Gibson, C. and Wright, J. (2001) 'Low self-control and coworker delinquency: A research note', *Journal of Criminal Justice*, vol. 29, no. 6, pp. 483-492.
23. Givon, M., Mahajan, V. and Muller, E. (1995) 'Software piracy: Estimation of lost sales and the impact on software diffusion', *The Journal of Marketing*, vol. 59, no. 1, pp. 29-37.
24. Gopal, R. D. and Sanders, G. L. (1998) 'International software piracy: Analysis of key issues and impacts', *Information Systems Research*, vol. 9, no. 4, pp. 380-397.
25. Gopal, R.D., Sanders, G.L., Bhattacharjee, S., Agrawal, M. and Wagner, S.C. (2004) 'A behavioral model of digital music piracy.' *Journal of Organizational Computing and Electronic Commerce*, vol. 14, no. 2, pp. 89-105.

26. Gottfredson, M. and Hirschi, T. (1987) 'The methodological adequacy of longitudinal research on crime', *Criminology*, vol. 25, no. 3, pp. 581-614.
27. Gottfredson, M. R. and Hirschi, T. (1990) *A general theory of crime,* Stanford University Press.
28. Gould, M. (2011) 'Kohlberg's Stages of Moral Development', *The Process of Socialization*, Salem Press, pp. 43-51.
29. Grasmick, H. G., Tittle, C. R., Bursik, R. J. and Arneklev, B. J. (1993) 'Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime', *Journal of Research in Crime and Delinquency*, vol. 30, no. 1, pp. 5-29.
30. Higgins, G. E. (2004) 'Can low self-control help with the understanding of the software piracy problem?', *Deviant Behavior*, vol. 26, no. 1, pp. 1-24.
31. Higgins, G. E. and Makin, D. A. (2004) 'Does social learning theory condition the effects of low self-control on college students' software piracy', *Journal of Economic Crime Management*, vol. 2, no. 2, pp. 1-22.
32. Higgins, G. E., Fell, B. D. and Wilson, A. L. (2006) 'Digital piracy: Assessing the contributions of an integrated self- control theory and social learning theory using structural equation modeling', *Criminal Justice Studies*, vol. 19, no. 1, pp. 3-22.
33. Higgins, G. E., Fell, B. D. and Wilson, A. L. (2007) 'Low self-control and social learning in understanding students' intentions to pirate movies in the United States', *Social Science Computer Review*, vol. 25, no. 3, pp. 339-357.
34. Higgins, G. E., Marcum, C. D., Freiburger, T. L. and Ricketts, M. L. (2012) 'Examining the role of peer influence and self-control on downloading behavior', *Deviant Behavior*, vol. 33, no. 5, pp. 412- 423.
35. Higgins, G. E. and Wilson, A. L. (2006) 'Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software', *Security Journal*, vol. 19, no. 2, pp. 75.
36. Higgins, G. E., Wolfe, S. E. and Marcum, C. D. (2008) 'Digital piracy: An examination of three measurements of self-control', *Deviant Behavior*, vol. 29, no. 5, pp. 440-460.

37. Hinduja, S., 2006. *Music piracy and crime theory.* LFB Scholarly Pub. LLC. P. 16.
38. Hinduja, S. and Ingram, J.R. (2009) 'Social learning theory and music piracy: The differential role of online and offline peer influences', *Criminal Justice Studies*, vol. 22, no. 4, pp. 405-420.
39. Hirschi, T. and Gottfredson, M. R. (1994) *The generality of deviance.* Transaction Publishers, pp. 23-47.
40. Hofstede, G., Hofstede, G. J. and Minkov, M. (1991) *Cultures and organizations: Software of the mind (Vol. 2).* McGraw-Hill, London.
41. Holt, T. J. and Copes, H. (2010) 'Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates', *Deviant Behavior*, vol. 31, no. 7, pp. 625-654.
42. Hsu, J. L. and Shiue, C. W. (2008) 'Consumers' willingness to pay for non-pirated software', *Journal of Business Ethics*, vol. 81, no. 4, pp. 715-732.
43. Husted, B. W. (2000) 'The impact of national culture on software piracy', *Journal of Business Ethics*, vol. 26, no. 3, pp. 197-211.
44. Ingram, J.R. and Hinduja, S. (2008) 'Neutralizing music piracy: An empirical examination', *Deviant Behavior*, vol. 29, no. 4, pp. 334-366.
45. Karaganis, J. (ed.), (2011) *Media Piracy in Emerging Economies,* United States of America: Social Science Research Council.
46. Kini, R.B., Ramakrishna, H.V. and Vijayaraman, B.S. (2003) 'An exploratory study of moral intensity regarding software piracy of students in Thailand.' *Behaviour & Information Technology*, vol. 22, no. 1, pp. 63-70.
47. Konstantakis, N.I., Palaigeorgiou, G.E., Siozos, P.D. and Tsoukalas, I.A. (2010) 'What do computer science students think about software piracy?', *Behaviour & Information Technology*, vol. 29, no. 3, pp. 277-285.
48. Kos Koklic, M., Vida, I., Bajde, D. and Culiberg, B. (2014) 'The study of perceived adverse effects of digital piracy and involvement: insights from adult computer users', *Behaviour & Information Technology*, vol. 33, no. 3, pp. 225-236.
49. Krueger, R. F., Caspi, A., Moffitt, T. E., White, J. and Stouthamer- Loeber, M. (1996) 'Delay of Gratification, Psychopathology, and Personality: Is Low Self- Control Specific to Externaiizing Problems?', *Journal of*

Personality, vol. 64, no. 1, pp. 107-129.

50. Kwong, K.K., Yau, O.H., Lee, J.S., Sin, L.Y. and Alan, C.B. (2003) 'The effects of attitudinal and demographic factors on intention to buy pirated CDs: The case of Chinese consumers', *Journal of Business Ethics*, vol. 47, no. 3, pp. 223-235.
51. LaRose, R. and Kim, J. (2006) 'Share, steal, or buy? A social cognitive perspective of music downloading', *CyberPsychology & Behavior*, vol. 10, no. 2, pp. 267-277.
52. Lau, E.K.W. (2003) 'An empirical study of software piracy.' *Business Ethics: A European Review*, vol. 12, no. 3, pp. 233-245.
53. Loch, K.D. and Conger, S. (1996) 'Evaluating ethical decision making and computer use', *Communications of the ACM*, vol. 39, no. 7, pp. 74-83.
54. Lalović, G., Reardon, S.A., Vida, I. and Reardon, J. (2012) 'Consumer Decision Model of Intellectual Property theft in Emerging Markets', *Organizations & Markets in Emerging Economies*, vol. 3, no. 1, pp. 58-74.
55. Longshore, D., Chang, E., Hsieh, S. C. and Messina, N. (2004) 'Self-control and social bonds: A combined control perspective on deviance', *Crime & Delinquency*, vol. 50, no. 4, pp. 542-564.
56. Luckenbill, D. F. and Miller, S. L. (1998) 'Defending intellectual property: State efforts to protect creative works', *Justice Quarterly*, vol. 15, no. 1, pp. 93-120.
57. Marron, D. B. and Steel, D. G. (2000) 'Which countries protect intellectual property? The case of software piracy', *Economic Inquiry,* vol. 38, no. 2, pp. 159-174.
58. Maruna, S. and Copes, H. (2005) 'What have we learned from five decades of neutralization research?', *Crime and Justice*, vol. 32, pp. 221-320.
59. Morris, R. G. and Higgins, G. E. (2010) 'Criminological theory in the digital age: The case of social learning theory and digital piracy', *Journal of Criminal Justice*, vol. 38, no. 4, pp. 470-480.
60. Morton, N.A. and Koufteros, X. (2008) 'Intention to commit online music piracy and its antecedents: an empirical investigation', *Structural Equation Modeling*, vol. 15, no. 3, pp. 491-512.

61. Peace, A.G., Galletta, D.F. and Thong, J.Y. (2003) 'Software piracy in the workplace: A model and empirical test', *Journal of Management Information Systems*, vol. 20, no.1, pp. 153-177.
62. Piquero, A.R. and Bouffard, J.A. (2007) 'Something old, something new: a preliminary investigation of Hirschi's redefined self- control', *Justice Quarterly*, vol. 24, no. 1, pp. 1-27.
63. Robins, R.W., Fraley, R.C. and Krueger, R.F. (eds.), (2009) *Handbook of research methods in personality psychology*. Guilford Press.
64. Siegfried, R.M. (2001, November) 'What's wrong with Napster? A study of student attitudes on downloading music and pirating software', *In Proceedings of the Infonnatrbn Systems Education Conference* (vol. 200).
65. Sheehan, B., Tsao, J. and Yang, S. (2010) 'Motivations for gratifications of digital music piracy among college students', *Atlantic Journal of Communication*, vol. 18, no. 5, pp. 241-258.
66. Shin, S. K., Gopal, R. D., Sanders, G. L. and Whinston, A. B. (2004) 'Global software piracy revisited', *Communications of the ACM*, vol. 47, no. 1, pp. 103-107.
67. Skinner, W. F. and Fream, A. M. (1997) 'A social learning theory analysis of computer crime among college students', *Journal of Research in Crime and Delinquency*, vol. 34, no. 4, pp. 495-518.
68. Sykes, G.M. and Matza, D. (1957) 'Techniques of neutralization: A theory of delinquency', *American Sociological Review*, vol. 22, no. 6, pp. 664-670.
69. Sykes, G. M. and Matza, D. (2003) 'Techniques of neutralization', in McLaughlin, E. et al. (eds.), *Criminological perspective: Essential readings*, Sage, pp. 231-238.
70. Sundararajan, A. (2004) 'Managing digital piracy: Pricing and protection', *Information Systems Research*, vol. 15, no. 1, pp. 287-308.
71. Taylor, S.A., Ishida, C. and Wallace, D.W. (2009) 'Intention to engage in digital piracy a conceptual model and empirical test', *Journal of Service Research*, vol. 11, no. 3, pp. 246-262.
72. Triandis, H. C. (1994) *Culture and Social Behavior*, McGraw-Hill Book Company, New York, NY, England.
73. Wall, D.S., 2010 'The Internet as a conduit for criminal activity. *Infor-*

mation Technology and The Criminal Justice System', Pattavina, A. (ed.), Sage Publications, pp.77-98.

74. Walls, W. D. (2008) 'Cross-country analysis of movie piracy', *Applied Economics*, vol. 40, no. 5, pp. 625- 632.
75. Wolfe, S.E. and Higgins, G.E. (2009) 'Explaining deviant peer associations: An examination of low self- control, ethical predispositions, definitions, and digital piracy', *W. Criminology Rev*., vol. 10, p. 43.
76. Wright, B. R., Moffitt, T. and Caspi, A. (1998, November) 'Predispositions, social environments, and crime: A model of varying effects'. In annual American Society of Criminology conference.
77. Yoon, C. (2011) 'Theory of planned behavior and ethics theory in digital piracy: An integrated model', *Journal of Business Ethics*, vol. 100, no. 3, pp. 405-417.
78. Zhang, L., Smith, W.W. and McDowell, W.C. (2009) 'Examining digital piracy: self-control, punishment, and self-efficacy', *Information Resources Management Journal (IRMJ),* vol. 22, no. 1, pp. 24-44.

b. Patents

Patent Evergreening: Law and Ethics

by Lisa P. Lukose[1]

1. Introduction

Intellectual property (IP) relates to knowledge and information which can be incorporated in tangible objects and can be commercially exploited. It is a collective term used to denote independent rights such as patents, trademarks, copyright, industrial designs, geographical indications, confidential information and layout designs activity in the industrial, scientific, literary and artistic fields. The nature, scope, content and duration of each right vary from property to property.[2] The main justifications for intellectual property rights (IPRs) are: protection of creator's rights as their creation stem from them[3]; protection of IP is an incentive to human creativity; it provides necessary stimulation for new Research and Development (R & D); it serves as an instrument for cultural, social, economic and technological development; new creativity helps create sustainable and competitive businesses locally and internationally; IP based industries contribute significantly to national economies and intellectual property right is a catalyst in the information technology development.

1 Associate Professor, University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University, Delhi, India.

2 For example, patent creates property rights in respect of novel inventions of first and true inventors for a period of 20 years whereas copyright confers property rights on independent creators of the original works for life time of the author plus 60 years. TRIPs Agreement provides the minimum period for which particular kinds of IPR should be protected in each member country; however, the member countries are at liberty to give longer protection.

3 See R. Spinello & M. Bottis, A defense of intellectual property rights, Edward Elgar Publishing, 2009.

2. Patents

Patent is one of the strong forms of IPRs. Countries give patent to reward new inventors. The patent law recognizes the exclusive right of a patentee to gain commercial advantage out of his invention. A patent[4] is an exclusive right granted by a country to the owner of an invention to make, use, manufacture and market the invention, provided the invention satisfies certain conditions stipulated in the law. This exclusive right granted on the patentee is only for a limited period of time. Exclusive right implies that no one else can make, use, manufacture or market the invention without the consent of the patent holder.

There are certain statutory criteria to be fulfilled to obtain a patent. Patent is an exclusive privilege to reward the true and first inventors of new inventions[5]. To qualify for patent protection, an invention must fall within the scope of patentable subject matter and must meet the three statutory requisites of novelty, inventive step and industrial application. This means that, to be patentable, an invention must be novel[6], non-obvious by involving an inventive step[7] and must be of industrial application[8]. The novelty requirement is, by and large, satisfied as long as the patent applicant was the first to invent the claimed invention[9]. The concept of novelty jurisprudence lays down that only what is new at the time of filing of the application for a patent is patentable. Novelty can be anticipated either by prior publication

4 Part II, section 5 of the TRIPS Agreement deals with Patents. The Patents Act, 1970 (infra referred to as the Act) regulates this area of law in India.

5 Under s. 2(1)(j), "invention" means a new product or process involving an inventive step and capable of industrial application.

6 As per s. 2 (1) (l) 'new invention' means any invention or technology which has not been anticipated by publication in any document or used in the country or elsewhere in the world before the date of filing of patent application with complete specification, *i.e.,* the subject matter has not fallen in public domain or that it does not form part of the state of the art.

7 Under s. 2(1)(ja), (ja) 'inventive step' means a feature of an invention that involves technical advance as compared to the existing knowledge or having economic significance or both and that makes the invention not obvious to a person skilled in the art.

8 S. 2(1)(ac) defines the phrase 'capable of industrial application'. In relation to an invention, it means that the invention is capable of being made or used in an industry.

9 *M/s Bishwanath Prasad Radhey Shyam* v. *Hindustan Metal Industries*, AIR 1982 SC 1444 at 1448.

or prior use. Mere discovery is not an invention. Patent is not granted for an idea or principle. To be the subject matter of a patent right, the article must be material and capable of being manufactured[10].

The requirement on industrial application suggests that the invention must be useful to the industry and it must serve some minimal human need. The condition on inventive step (non-obviousness) requirement denies patentability if the differences between the claimed invention and the relevant prior art are such that the claimed invention would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains.

The invention may be a product or process and its scope extends to all fields of technology[11]. The inventor, in order to obtain protection, has to disclose the invention and also describe the method of performing it. The patent confers on the patentee the right to exclude others from, among other things, making, using or selling the invention.

Countries may exclude from patentability certain inventions to protect *ordre public* or morality or to protect human, animal or plant life or health or to avoid serious prejudice to the environment, provided that such exclusion is not made merely because the exploitation is prohibited by such countries' municipal laws[12].

The object of patent law is to encourage scientific research, new technology and industrial progress[13]. The patent system is premised on the reasonable assumption that the public will enjoy additional benefits when the government takes additional steps to encourage the creation, commercialization, and disclosure of new inventions. The basic argument is that the society benefits when people conceive of new inventions, develop and commercialize new products incorporating these inventions and publicly disclose information about their inventions, so that others may learn from

10 In *Diamond* v. *Chakrabarty,* 447 U.S. 303 (1980) it was held that the touchstone of patentabilty is not whether an invention involves living or inanimate subject matter but whether it involves a human made invention.

11 Article 27. 1 of TRIPS.

12 See, article 27. 2 of the TRIPS Agreement and section 3 of the Indian Patent Act, 1970.

13 Peter G. Groves, *Source Book on Intellectual Property Law*, Cavendish Publishing Ltd., London, 1997. On protection of inventor's rights, as inventions come from their skill and labor, see Spinello & Bottis, above.

and improve upon these inventions. Inventing something new often requires a substantial investment of intellect, time and capital. The technology disclosed serves to stimulate ideas for further invention and innovation. The economic value of patent information is that it provides industry with technological information that can be used for commercial purposes. If there is no protection, there may be a substantial incentive to take a free ride on someone else's investment. This potential for free-riding reduces the incentive to invent something new because the inventor may be unable to recoup the investment.

Patents are also meant to correct a market failure. The market failure leads to sub-optimal levels of investment in innovative activities and arises because producers that can use an innovation without incurring research and development costs will always have a competitive advantage over firms that innovate and incur those costs. As a result, there will be no incentive to innovate. Patents reward innovators with a temporary monopoly on the intellectual property that they have created[14]. The patent holder is required to disclose the scientific knowledge that underlines the innovation to the public in order to promote knowledge dissemination. Making the scientific information available instead of allowing it to remain proprietary has the objective of reducing information costs for other innovators.

Thus, patent confers property rights on inventors of new inventions. Among all forms of IPRs, the patent is considered to be the most economically potential form of IPR which has direct impact on scientific and technological development of a country and which considerably influences the public health policy of a nation[15].

As the discussions above reveal, an invention *per se* may not be patentable notwithstanding it satisfies the triple test of patentability[16]. The inven-

14 In *Raj Parkash* v. *Mangat Ram Chowdhry and Ors.*, AIR1978 Delhi1, it was observed that the grant of patent, no doubt, creates a monopoly in favor of the patentee but then law throughout the free world recognizes that an inventor must first get the benefit of his invention, even if it means creating a monopoly.

15 N. Rajagopala Ayyangar Committees' Report–1957 unequivocally stated thus: "It would not be an exaggeration to say that the industrial progress of a country is considerably stimulated or retarded by its patent system".

16 Arts. 27.2 & 27.3 of TRIPS Agreement provide thus:
27. 2. Members may exclude from patentability inventions, the prevention within

tion must not have been excluded from patentability, *i.e.,* the subject matter of the patent must not be a non-patentable invention in the country concerned. TRIPS Agreement provides enough flexibility for its member countries under clauses 2 and 3 of article 27 to exclude certain inventions form patentability *inter alia* to protect *ordre public* or morality or to protect human, animal or plant life or health. Every country has thus the right to exclude from patentability certain inventions on these permissible grounds. In India, section 3 of the Indian Patent Act has been amended to provide for non-patentable inventions. It enlists the inventions that are not patentable though otherwise they may fulfil the prerequisites for patents.

3. The real objective of patents

Section 83 of the Patent Act makes it crystal clear that the patents are not granted merely to enable patentees to enjoy a monopoly. The section reads that:

a) that patents are granted to encourage inventions and to secure that the inventions are worked in India on a commercial scale and to the fullest extent that is reasonably practicable without undue delay;
b) that they are not granted merely to enable patentees to enjoy a monopoly for the importation of the patented article;
c) that the protection and enforcement of patent rights contribute to the promotion of technological innovation and to the transfer and

their territory of the commercial exploitation of which is necessary to protect *ordre public* or morality, including to protect human, animal or plant life or health or to avoid serious prejudice to the environment, provided that such exclusion is not made merely because the exploitation is prohibited by their law.
3. Members may also exclude from patentability:
(a) diagnostic, therapeutic and surgical methods for the treatment of humans or animals;
(b) plants and animals other than micro-organisms, and essentially biological processes for the production of plants or animals other than non-biological and microbiological processes. However, Members shall provide for the protection of plant varieties either by patents or by an effective *sui generis* system or by any combination thereof. The provisions of this subparagraph shall be reviewed four years after the date of entry into force of the WTO Agreement.

dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations;

d) that patents granted do not impede protection of public health and nutrition and should act as instrument to promote public interest specially in sectors of vital importance for socio-economic and technological development of India;
e) that patents granted do not in any way prohibit Central Government in taking measures to protect public health;
f) that the patent right is not abused by the patentee or person deriving title or interest on patent from the patentee, and the patentee or a person deriving title or interest on patent from the patentee does not resort to practices which unreasonably restrain trade or adversely affect the international transfer of technology; and
g) that patents are granted to make the benefit of the patented invention available at reasonably affordable prices to the public. They are not granted to impede protection of public health but the patent should act as instrument to promote public interest especially in sectors of vital importance for socio- economic and technological development of India.

While going by section 83, one can understand that there are many practices primarily being practiced by developed nations in order to obtain patents which are against the interest of the developing and least developing world. Such practices include bio-piracy, traditional knowledge misappropriation, ever greening etc. In the past decades the patent system has been subjected to different types of misuse such as patent ever-greening, patent trolling, patent thicketing etc., all these practices have caused serious damage to innovators, technology producers, and of course, the general public[17]. The remaining part of the article shall focus on evergreening and its impact on poor countries.

17 Nagaraj Mannikeri and Vidya Bhaskar Singh, *Patent Trolling And Evergreening: Unethical Acts Or Malpractices?*; at http://www.foxmandal.com/wp-content/uploads/2015/06/Malpractices-in-the-Patent-system-final-June-15-21.pdf.

4. Patent evergreening

Ever-greening of patent is an abuse and misuse of patent system. It is the perpetual renewal of patents. It denotes lifecycle management the practice of pharma companies seeking extra patents on minor variations of the original drug – new forms of release, new dosages, new combinations or variations, or new forms, changing a drug from a tablet to a capsule etc. In this process, a trifling change is made to an existing product and later it will be claimed as a new invention. Drug companies generally do evergreening, by filing new patent applications, tweaking existing molecules to show novelty. Evergreening of patent is a phrase used to label practices that have developed in certain jurisdictions wherein a trifling change is made to an existing product, and claimed as a new invention. The coverage/protection afforded by the alleged new invention is then used to extend the patentee's exclusive rights over the product, preventing competition. These changes are typically made to blockbuster drugs shortly before their patents expire. Evergreening is possible in many countries like Australia and US because their legal standard required to get a patent is very low. Different methods of delivering drugs (such as extended release, for example) have been known for decades. But when one of these known delivery methods is combined with a known drug, the patent office considers this sufficiently inventive to grant a new 20-year patent[18]. New use patents directly or indirectly supports evergreening in the developed nations. Low standard benchmark set by the US for inventive steps and utility, allows trivial drug patents. National Institute of Health Care Management on Pharmaceutical Innovation reports that over 75% of the patented drugs are new forms of known substances, thus eliminating competition, extending monopolies, making drugs unaffordable and adversely affecting the right to health[19].

The negative impacts of evergreening are many. Evergreening extends the period of market exclusivity. It forces the generic manufacturer to wait indefinitely for all the patents to expire and delays the introduction of generic competition. It adversely impacts public health and plays a detri-

18 http://theconversation.com/explainer-evergreening-and-how-big-pharma-keeps-drug-prices-high-33623.

19 2002 Report.

mental role in driving out the domestic generic medicine market which provides access to vital medicinal or life saving drugs at affordable prices to lower section of the society. For example, the patented drug 'Gleevec' costed in India Rs. 4,115/- per tablet. Its generic version is being sold in India by Resonance and Indian generic drug company at Rs. 30/- per tablet. While the annual cost of the Gleevec is Rs.15,00,000/-[20] in India its generic versions costs just Rs.10,000/- annually. On the expiry of patents for a widely used drug, the price falls up to 95%.[21] Allowing patents for new use of pharmaceuticals directly or indirectly encourages ever-greening in the developed nations.

5. Public health vis-a-vis patents

Right to health is a fundamental right of every human being. WHO Constitution encourages the member states to achieve highest attainable standard of health. The human right to health implies that everyone has the right of physical and mental health, which includes access to all medical services, sanitation, adequate food, decent housing, healthy working conditions, and a clean environment. It is not an utopian notion of right to be healthy. On the contrary, it means that the state has to generate conditions in which everyone can be as healthy as possible. These conditions include ensuring availability of health services, healthy and safe working conditions, adequate housing and nutritious food.

The right to health contains four elements:[22] *Availability* - Adequate functioning public health care facilities, goods and services, as well as programmes should be available in all geographical areas and to all communities; *Accessibility* - Access to health facilities, goods and services must be universal, guaranteed for all on an equitable basis. Accessibility has four overlapping dimensions: Non-discrimination, Physical accessibility, Economical accessibility (affordability) and Accessibility of information; *Ac-*

20 Novartis ranked in a total turnover of US $ 1.69 billion from US alone in 2012 from the drug, Gleevec.

21 http://theconversation.com/explainer-evergreening-and-how-big-pharma-keeps-drug-prices-high-33623.

22 UN General Comment on the Right to Health in 2000.

ceptability - All health facilities, goods and services must respect medical ethics. They must respect dignity, provide culturally appropriate care, be responsive to needs based on gender, age, culture, language, and different ways of life and abilities; and *Quality*: - Health facilities, goods and services must be scientifically and medically appropriate and of good quality.

As per section 83 of the Indian Patent Act, patents should not impede protection of public health but the patent should act as instrument to promote public interest especially in sectors of vital importance. However, in reality, the existing patent practices are prejudicial to the public health especially in the developing and least developing countries.

6. Pharmaceutical patents and public health issues

Pharmaceutical patents are designed to stimulate investment in new lines of R & D. However, there is no exaggeration in stating that the product patent regime in pharmaceutical products, directly or indirectly, creates private monopolies encouraging evergreening of patents, resulting in patent abuse affecting the human rights of millions of patients in low income countries, facilitating giant multinational pharmaceutical companies to artificially extend the period of patent to keep competitors out and keep the prices of the patented product high. For example, coincidently, in the parliamentary debates on the amendment of the patent law in 2005 to comply with the TRIPS requirements by shifting from the regime of process patents to product patents in pharmaceuticals etc., there has been reference to the 'Novartis' and the medicine 'Gleevec/Glivec' and how Novartis has excessively high priced the drug after the grant of EMR.

India has played a very significant role in the pre-TRIPS regime as the producer and supplier of drugs to different parts of the world where impoverished humanity was critically in need of drugs at cheap and affordable prices. India has been the leader in the global supply of affordable antiretroviral drugs and other essential medicines prior to the conclusion of TRIPs Agreement. It was supplying 50 per cent of the cheapest drugs in the world to places like Papua New Guinea, Laos, Kenya, Africa, *etc*. India has also taken leadership in promoting access to and supplying affordable essential generic HIV medicines to those most in need in developing countries. As the countries worst hit by AIDS do not have sufficient manufacturing

capacity in the pharmaceutical sector, they rely upon imports from major generic drugs producing countries such as India for HIV treatment of the millions of their patients.

However, the TRIPS Agreement required crucial legislative changes mandating product patent which had aroused grave concerns about its impact on public health. It also had raised concern on the impact of TRIPS' drugs patent regime on the local production and supply of generic antiretroviral agents. India had learnt from experience the inverse relationship between product patents and the indigenous pharmaceutical industry, and its effects on the availability of essential drugs at affordable prices. When India had a product patent regime, we had to depend upon imports for the 85 per cent of our medicinal requirements. This situation was reversed when we shifted to process patent regime, i.e., 85 per cent of India's medicinal requirement was met by our own products. From 1970 after the patent system in India barred the grant of product patents for pharmaceutical and chemical substances, the pharmaceutical industry in the country scaled great heights and became the major supplier of drugs at cheap prices to a number of developing and under developed countries. After studying the situation in and experience of other countries and recommending India to introduce process patent system, Justice Ayyangar said thus:[23]

> *"I have considered the matter with the utmost care and have reached the conclusion that the chemical and pharmaceutical industry of this country would be advanced and the tempo of research in that field would be promoted if the German system of permitting only process claims were adopted."*

During the process patent regime, India has benefited from the low cost generic industry to dominate 30 per cent of the low cost drugs in the world. India was a large supplier of generic antiretroviral drugs to several countries such as Ghana, Lesotho, Malawi, Namibia, Bangladesh, Cambodia,

23 Justice Ayyangar observed that the provisions of the Patent law have to be designed, with special reference to the economic conditions of the country, the state of its scientific and technological advancement, its future needs and other relevant factors, and so as to minimize, if not to eliminate, the abuses to which a system of patent monopoly is capable of being put. See, N. Rajagopala Ayyangar Committees' Report – 1957.

China, Indonesia, Korea, Laos, Thailand, Papua New Guinea, Vietnam *etc*.

On 01.01.2005, to comply with the TRIPS requirements India had to shift again from the process patent regime to product patent regime in medicines, agricultural and chemical substances. However, to prevent the abuse of product patent several changes were introduced in the 2005 amendment including pre-grant oppositions[24], amendments in section 3 widening the scope of non-patentable inventions and redrafting of section 3(d). Amendment in section 3(d) was the most crucial amendment directly preventing ever-greening of pharma patents and checking attempts for repetitive patents.

7. Section 3 (d) – Non patentable inventions and the *Novartis* case

Section 3 of the Indian Patent Act deals with non-patentable inventions. A close look at the Indian Patent Act, as it stands today clarifies that "invention" and "patentability" are two distinctly separate concepts. This is a vital distinction which is at the heart of the Indian Patent Act. The duality of the two concepts is best understood from the concepts of 'non patentable inventions'. For grant of a statutory patent in India, like any other jurisdiction, the subject matter must satisfy the twin tests of "invention" and "patentability". The test of 'invention' is satisfied if it fulfils the three prerequisites of patentability-novelty, inventive step and industrial utility as discussed above. Something may be an "invention" as the term is generally understood and yet it may not qualify as an "invention" for the purposes of the Act. Further, something may even qualify as an "invention" as defined under the Act and yet may be denied patent for other large considerations/ public interest as may be stipulated in the Act.

The most controversial section among the non-patentable clauses is the section 3(d). The section 3 (d) after 2005 amendment reads thus: "The mere discovery of a new form of a known substance which does not result in the enhancement of the known efficacy of that substance or the mere discovery of any new property or new use for a known substance or of the mere use of a known process, machine or apparatus unless such known process results

24 S. 25 (1).

in a new product or employs at least one new reactant." The *Explanation* to section 3(d) sates thus: For the purposes of this clause, salts, esters, ethers, polymorphs, metabolites, pure form, particle size, isomers, mixtures of isomers, complexes, combinations and other derivatives of known substance shall be considered to be the same substance, unless they differ significantly in properties with regard to efficacy". Section 3 (d) of the erstwhile Patent Act before 2005 amendment which reads: "The mere discovery of any new property or mere new use for a known substance or of the mere use of a known process, machine or apparatus unless such known process results in a new product or employs at least one new reactant". As evidenced, there is, in the amended provision, an addition of the opening words in the substantive provision and the insertion of explanation to the substantive provision. It adds the words "the mere discovery of a new form of a known substance which does not result in the enhancement of the known efficacy of that substance or" at the beginning of the provision; and deletes the word "mere" before "new use". It also adds an explanation at the end of the clause.

8. Novartis A. G. v. Union of India

Jürg Zimmermann invented a number of derivatives of N-phenyl-2- pyrimidineamine, one of which is CGP 57148 in free base form (later given the International Non-proprietary Name '*Imatinib*' by the World Health Organisation). These derivatives, including Imatinib2, are capable of inhibiting certain protein kinases, especially protein kinase C and PDGF (platelet-derived growth factor)-receptor tyrosine kinase and thus have valuable anti-tumour properties and can be used in the preparation of pharmaceutical compositions for the treatment of warm-blooded animals, for example, as anti-tumoral drugs and as drugs against atherosclerosis. The N-phenyl-2-pyrimidine-amine derivatives, including Imatinib, were granted patent on 28.05. 1996 (US Patent No. 5,521- the Zimmermann Patent). The Zimmermann compounds (i.e., derivatives of N-phenyl-2-pyrimidine-amine) were also granted a European patent (Patent No. EP-A-0 564 409).

An application was filed subsequently in India (Application No.1602/MAS/1998) for grant of patent for Imatinib Mesylate in beta crystalline form at the Chennai Patent Office on 17.07. 1998 in which it was claimed that the invented product, the beta crystal form of Imatinib Mesylate, has

(i) more beneficial flow properties: (ii) better thermodynamic stability; and (iii) lower hygroscopicity than the alpha crystal form of Imatinib Mesylate. It further claimed that the aforesaid properties makes the invented product "new" and superior as it "stores better and is easier to process;" has "better processability of the methanesulfonic acid addition salt of a compound of formula I", and has a "further advantage for processing and storing". In short, Novartis filed an application before the Chennai patent office related to a drug name GLIVEC which was slightly a different version of its 1993 patent for Anti Leukaemia drug.

Before the application for patent was taken up for consideration, the appellant made an application (Application No. EMR/01/2002) on 27.03.2002, for grant of exclusive marketing rights (EMR)[25] under erstwhile section 24A of the Patent Act and on 10.11.2003 EMR was granted. The patent applica-

25 TRIPS required that WTO member countries not having provision in their laws for granting product patents in respect of drugs and agrochemical, must introduce during the transition period, Exclusive Marketing Rights (EMR) for such products, if the following criteria are satisfied: (i) A patent application covering the new drug or agrochemical should have been filed in any of the WTO member countries after 01.01.1995; (ii) A patent on the product should have been obtained in any of the member countries (which provides for product patents in drugs and agrochemical) after 01.01.1995; (iii) Marketing approvals for the product should have been obtained in any of the member countries;(iv) A patent application covering the product should have been filed after 01.01.1995 in the country where the EMR is sought; and (v) The applicant should apply seeking an EMR by making use of the prescribed form and paying requisite fee. EMR was valid only up to a maximum period of 5 years or until the time the product patent laws came into effect. EMR provided exclusive marketing rights to sell or distribute the article or substance covered in a patent application. The purpose of EMRs was to ensure that the innovator can market free copies of his product. In India the EMR was made applicable *w. e. f.* 01.01.1995. A new Chapter IVA has been added by The Patents (Amendment) Act, 1999 with retrospective effect from 01.01. 1995 to provide for the EMR. EMR's are intended to be a transitory device, until process patent jurisdi1ctions migrate to a full product patent regime. An EMR application lies only if the corresponding patent application is already in the mailbox. Also see Sangeeta Vohra, "Understanding Exclusive Marketing Rights as a Species of Patents" available at http://www.algindia.com/publication/article1200.pdf, visited on 01.12.2013. When India entered in the full fledged product patent regime on 01.01.2005 as per art. 65 of TRIPS agreement exclusive marketing rights have been abolished by omitting chapter IVA from the Patents Act. The EMRs granted before 01.01.2005 continued to enjoy the same terms and conditions on which it was granted.

tion was taken out of the "mailbox" for consideration only after amendments were made in the Patents Act, with effect from January 1, 2005. By that time the application had attracted five pre-grant oppositions in terms of section 25(1) of the Act. On 15.12.2005 the Assistant Controller of Patents and Designs rejected the application for grant of patent under section 3(d) holding *inter alia* that (i) the invention claimed by the appellant was anticipated by prior publication, i.e. the Zimmermann patent and (ii) the invention claimed by the appellant was obvious to a person skilled in the art in view of the disclosure provided in the Zimmermann patent specifications. Against the orders a writ was filed in the Madras High Court. Novartis prayed the Court to declare section 3(d) of Patent (Amendment) Act 2005 non compliant with the TRIPS Agreement and violative of Article 14 of the Constitution. The argument on Article 14 of the Constitution of India was based on arbitrary discretionary power vested in the Patent Controller in determination of enhanced efficacy.

The high court of Madras upheld the constitutional validity of section 3(d) by holding that 'efficacy' means 'therapeutic efficacy'. While dismissing the writ petitions assailing section 3(d) of the Act, the High Court observed thus: "When the Appellant was holding the right as EMR on GLEEVEC it used to charge Rs.1,20,000/- per month for a required dose of the drug from a cancer patient, not disputed by the Appellant, which in our view is too unaffordable to the poor cancer patients in India. Thus, we also observe that a grant of product patent on this application can create a havoc to the lives of poor people and their families affected with the cancer for which this drug is effective. This will have disastrous effect on the society as well. Considering all the circumstances of the appeals before us, we observe that the Appellant' alleged invention will not be worthy of a reward of any product patent on the basis of its impugned application for not only for not satisfying the requirement of section 3(d) of the Act, but also for its possible disastrous consequences on such grant as stated above, which also is being attracted by the provisions of section 3(b) of the Act which prohibits grant of patent on inventions, exploitation of which could create public disorder." The Court said that the Amendment was intended to preventing evergreening; to provide easy access to the denizens of this country for life saving drugs; and to discharge their constitutional obligation of providing health care to its citizens.

On the same matter, the Intellectual Property Appellate Board (IPAB), held that the patentability of the subject product was regulated by section 3(d) of the Act.[26] The order of the IPAB clearly stated that "since India is having a requirement of higher standard of inventive step by introducing the amended section 3(d) of the Act, what is patentable in other countries will not be patentable in India. The object of amended section 3(d) of the Act is nothing but a requirement of higher standard of inventive step in the law particularly for the drug/pharmaceutical substances."

The IPAB's order was challenged in the Supreme Court in a petition under article 136 of the Constitution. The court examined at length the section 2(1)(j) defining invention as "a new product or process involving an inventive step and capable of industrial application" and section 2(1)(ja) defining inventive step as "a feature of an invention that involves technical advance as compared to the existing knowledge or having economic significance or both and that makes the invention not obvious to a person skilled in the art," and held that Imatinib Mesylate did not qualify the test of 'invention' as laid down in the above provisions.

On appeal, the Supreme Court of India disapproved the contention that section 3(d) is a provision *ex majore cautela* and is an exception to clauses (j) and (ja) of section 2(1) of the Act. According to the court, the amended portion of section 3(d) clearly sets up a second tier of qualifying standards for chemical substances/pharmaceutical products in order to leave the door open for true and genuine inventions but, at the same time, to check any attempt at repetitive patenting or extension of the patent term on spurious grounds. By giving a purposive interpretation of sub sections (j) and (ja) of section 2(1) with section 3(d) the court held that the Act sets different standards for qualifying as "inventions" things belonging to different classes, and for medicines and drugs and other chemical substances, the Act sets the invention threshold further higher, by virtue of the amendments made in section 3(d) in the year 2005.

The Supreme Court held that both the Zimmeman patent and the new

26 Though agreeing with the Assistant Controller that no product patent for the subject patent could be allowed in favour of the appellant, the IPAB held that the appellant could not be denied the process patent for preparation of Imatinib Mesylate in beta crystal form.

claimed substance - are basically one and the same. Regarding the issue of 'efficacy' the court observed that the test of efficacy would depend upon the function, utility or the purpose of the product under consideration. In the case of a medicine that claims to cure a disease, the test of efficacy can only be 'therapeutic efficacy'. The court was of the view that the 'therapeutic efficacy' of a medicine must be judged strictly and narrowly. On the issues of 'enhancement of the known efficacy' and the explanation that requires the derivative to 'differ significantly in properties with regard to efficacy', the court stated that not all advantageous or beneficial properties are relevant, but only such properties that directly relate to efficacy, which in case of medicine, is its therapeutic efficacy. The mere change of form with properties inherent to that form would not qualify as 'enhancement of efficacy' of a known substance. This explains what is not to be considered as therapeutic efficacy.

9. Moral of the case

The *Novartis* case thus gives a clear indication that India would no longer permit ever greening of patents risking public health and at the cost of poor patients in the country. The judgment gives a strong message to the world that India will give pharmaceutical companies extended market monopoly only of a medicine is genuinely innovative and involves substantive innovation. The decision preempts pharma companies to seek evergreening of patents in India by extending patent on known drugs and the consequent delay on the availability of affordable generic versions. It would certainly facilitate early entry of generic medicines into the market for other medicines too. The impact would be felt not only in India but also across the developing world that depend on Indian generic versions. *Novartis* is a precedent for other countries as well in determining the patentability of 'minor improvements.' No legal system should permit the artful drafting of claims by giant pharma companies to decide the scope of patent law. The judgment itself says: "We certainly do not wish the law of patent in this country to develop on lines where there may be a vast gap between the coverage and the disclosure under the patent; where the scope of the patent is determined not on the intrinsic worth of the invention but by the artful drafting of its claims by skilful lawyers, and where patents are traded as a

commodity not for production and marketing of the patented products but to search for someone who may be sued for infringement of the patent."

10. Conclusion and suggestions

It is estimated that more than 8,000 people around the world die every day because they lack of access to treatment. Only about one in ten people in urgent need of HIV antiretroviral treatment in 'low and middle income' countries has access to existing medicines. Patents are needed to encourage innovations. The patent system provides necessary incentives for investment in research and encourages inventors to engage in new lines of R & D, thus it stimulating further creativity. At the same time, there should be vital areas like public health, which should be the paramount consideration and countries must use TRIPS flexibility to exclude/revoke patents to protect public health.

The Novartis court was not against patent law. The Novartis judgement does not violate to patent laws. The court considered only public interest and public health while deciding the case. The right to health is a cause of concern in many parts of the world. One-third population of the world does not have access to basic medicines and among this one-third, majority of population lives in African and Asian continent. Since price is one of the major factors in accessibility, this decision was of great significance as it allowed many poor countries to access the patented drug at affordable prices[27].

The need of the hour is to create balance between the *patents and the patients*-a balance between the patent laws and public health considerations, so that drugs are affordable by the common people. Availability and affordability of drugs must be considered as two sides of the same coin. Check and balances in the Patent system including TTRIPS flexibilities, exclusion from patentability, compulsory licensing etc. must be boldly evoked by countries to address public health issues. Article 27.2 of The TRIPS Agreement itself provides that "members may exclude from patentability inventions, the prevention within their territory of the commercial exploitation of which is necessary to protect *ordre public* or morality, including to pro-

27 http://www.lawctopus.com/academike/evergreening-an-abuse-of-the-patent-system/.

tect human, animal or plant life or health or to avoid serious prejudice to the environment, provided that such exclusion is not made merely because the exploitation is prohibited by their law".

The countries must penalise evergreening practices by making necessary amendments in their patent laws. For instance, Australian patent law provides safeguards against ever-greening by imposing penalties under sections 26C and 26D of Australian Patent Act, 1990. The Act also has a mechanism for damages to be paid to the government if ever-greening practices are proved. Similarly, Article 18.9.4 of the Republic of Korea-United States Free Trade Agreement (KORUSFTA) has been specifically drafted to permit the establishment of pharmaceutical patent "anti-evergreening" oversight agency[28].

Evergreening of patents is against the scheme and spirit of patents and it is highly unethical. Patents should not result in non-availability and non-affordability of medicines. Developing and least developing world must take *Novartis* as a case study to understand how the TRIPS flexibilities can be used against unethical evergreening of patents.

11. References

1. Amato, A. D', and Long, D. E. (eds.), *International Intellectual Property Law*, Kluwer Law International, 1997.
2. Bainbridge, D. I., *Intellectual Property,* Longman Publishing, 2010.
3. Black, T., *Intellectual Property in Industry*, Butterworth & Co, (Publishers) Ltd, 1989.
4. Cornish, W. R., *Intellectual Property, Patents, Copyright, Trademarks And Allied Rights*, Universal Law Publishing Co Pvt, Ltd. (for developing countries).
5. Verky, E. *Law of Patents*, Eastern Book Co., 2005.
6. Groves, P. J., *Source Book on Intellectual Property Law*, Cavendish Publishing Ltd.

28 http://www.foxmandal.com/wp-content/uploads/2015/06/Malpractices-in-the-Patent-system-final-June-15-21.pdf

7. Bently, L. and Sherman, B., *Intellectual Property Law*, Oxford University Press, Oxford, 2003.
8. LTC Harms, *The Enforcement of Intellectual Property Rights*: *A Casebook*, WIPO, Geneva, 2005.
9. Narayan, P., *Intellectual Property Law*, Eastern Law House, 2002.
10. Shiva, V., *Patents: Myths & Reality,* Penguin Books, New Delhi, 2001.
11. Watal, J., *Intellectual Property Rights in WTO & Developing Countries,* Oxford University Press, New Delhi, 2001.
12. Spinello, R., and Bottis, M., *A defense of intellectual property rights*, Edward Elgar Publishing, 2009.

E - COMMERCE

Emerging Issues in Electronic Contracting in the Laws of South Africa and Namibia where one Party is a "Robot"

by Aimite Jorge[1]

1. Introduction

So far in our legal systems, both South Africa and Namibia, we maintain that a contract is an agreement between at least two people, let them be "A" & "B". In the traditional and simplistic form, a formation of contract starts like this: "A" offers something to "B" (to contract with "B") and "B" accepts the offer. The contract comes into existence once both minds meet. "A" and "B" are normally assumed to be either "natural persons" or Juristic persons. Even in the case of juristic person, "A" and "B" are usually represented by natural persons. The expression of intention of one person "A" to contract with another "B" is accepted by "B" and the contract is formed. The law also has so far accepted the contract concluded between "A" and "B" who are not in the presence of each other. Traditionally, information theory applies to these contracts; in some cases the expedition theory (mail-box rule) and in limited occasions, the reception theory (see example, South African Electronic Communication Act, sec. 22 and 23) applies.

In recent times, however, the evolution and combined use of computers and telecommunications, and the latest evolution in the field of Artificial Intelligence (AI) have brought a new dimension to the process of contracting. These developments have also brought new dimensions to the process of expressing the will and declaration of intentions. The new modern process of contracting increasingly uses what is called "intelligent electronic

1 University of Namibia & University of Cape Town, Private Law Department.

agents". In the field of contracting through intelligent electronic agents, there is an imperious need to analyzing the question of expression of consent. One of the main questions that arises in this area is "how far we can go in considering computer intelligence and autonomy. Said differently, how can we legally deal with a new form of electronic behavior of autonomous actions?

In the process of analyzing the expression of consent, two possibilities may arise:

One is that electronic devices that mediate human consent should be considered as mere machines or tools in the process of consenting;

The second possibility is that such electronic devices should be considered" by analogy" as legal persons.

2. Conceptual understandings

2.1 What is an electronic intelligent agent?

The concept of agent can be divided into a "single agent" and "multiple-agents".

2.1.1 The concept "agent" per se

The concept agent *per se* traditionally means "one who agrees and authorized to act on behalf of another, a principal, to legally bind an individual in particular business transactions with third parties pursuant to an agency relationship.

2.1.2 Concept agent in computer related language and electronic telecommunications

It is in this field of computer language studies and electronic telecommunications that mostly the concept of agent (and intelligent agent) is often used nowadays. In this field of studies the concept does have a dual meaning of "single agent" and "multiple agents". In this area of studies, these agents are commonly known as 'software agents" and lately also as "intelligent electronic agents". The basic attributes of a software agent are that these agents:

- are not strictly invoked for a task, but activate themselves
- may reside in wait status on a host, perceiving context
- may get to run status on a host upon starting conditions

- do not require interaction of user
- may invoke other tasks including communication.[2]

Nevertheless, in computer-related language, there is no uniform definition for an agent: Casual definitions of agents can be "a software thing that knows how to do things that you could do probably yourself if you had the time" (Hermans 1996). Other studies present an alternative classification based on agent-mediated e-commerce. In short some of these studies describe agents as software tools that have the following functions and characteristics:

- social ability: agents interact with other agents or individuals
- reactivity: agents respond to changes that occur in their environment
- pro-activity: agents are programmed to pursue goal directed behavior
- adaptivity: agents assimilate to the user's habits and benevolence assuming that they do not have conflicting goals, and
- mobility: some agents can move in an electronic environment, in our case the Internet.

As to pure electronic agents, there are at least four modes of perceiving an electronic intelligent agent. One is a neutral mode; the other is a weak mode, and the third as a strong mode:

On the neutral mode, an agent is anything that can be viewed as perceiving its environment through sensors and acting upon that environment through effectors."[3]

On the slightly weak mode, an agent[4] is one that has at least some of the following characteristics:

- autonomy: agents operate without direct intervention of humans,

2 Jennings, N. R., Varga, L. Z., Aarnts, R. P., Fuchs, J. & Skarek, P. (1993), "Transforming Stand-Alone Expert Systems into a Community of Cooperating Agents", in *International Journal of Engineering Applications of Artificial Intelligence* 6(4), pp. 317-331, p. 320.

3 Russell and Norvig (1995) "*Artificial Intelligence: a Modern Approach*", Prentice Hall, Boston, p. 651.

4 Woodridge and Jennings "Essential properties of an Agent".

and have control over their actions and internal state

- social ability: agents interact with other agents (and possibly humans) via an agent communication language
- reactivity: agents perceive their environment and respond in a timely and rational fashion to changes that occur in it
- pro-activeness: agents do not simply act in response to their environment, they are capable of taking the initiative (generate their own goals and act to achieve them).

In the stronger notion, the agent is perceived as having mental properties, such as knowledge, belief, intention, obligation. In addition, and agent has other additional properties such as:

- mobility: agents can move around from one machine to another and across different system architectures and platforms
- veracity: agents do not knowingly communicate false information
- benevolence: agents always try to do what they are asked of
- rationality: agents will try to achieve their goals and not act in such a way to prevent their goals from being achieved.

The fourth notion of the agent is inter-inclusive. On this notion, "intelligent agents" are described as software entities that carry out some set of operations on behalf of a user or another program with some degree of independence or autonomy, and in so doing, employ some knowledge or representation of the user's goals or desires (from IBM).

2.2 Concept of multi-agents

In computer and telecommunication environments, the concept "multi-agent" refers to a system that consists of agents and their environment. The concept is used in search engines, e-commerce and beyond. Typically in these fields, "multi-agent" systems research refers to software agents. A software agent is a computer analog of an autonomous robot. Thus, software agents represent an evolutionary step beyond conventional computer programs. Software agents can activate and run themselves, not requiring inputs or interaction with a human user. Consequently "software agents" are essentially robots and are often "intelligent robots" or 'semi-intelligent

agents".

However, the agents in a multi-agent system could equally well be all robots, humans or human teams. A multi-agent system may contain combined human-agent teams (meaning "humans and 'robots teams".

With this conceptualization in mind, agents can then be divided into different types and categories, ranging from simple to complex agents. Nevertheless the operation of all agents will at least fall within these three main fields: DAI, PAI, and DPS. DAI stands for "distributed-artificial-Intelligence"; PAI stands for "parallel-artificial-intelligence" and DPS stands for "distributed-problem-solving". Historically, the concept DAI "distributed-artificial-intelligence" is slightly older than the other concepts. It evolved from the 1970s in the words of Carl Hewitt[5] in which he studied the concurring actor model. In this model of the agent, that Carl Hewitt had already proposed the concept of a self-contained, interactive and concurrently-executing object which he termed "ëactori". This object had some encapsulated internal state and could respond to messages from other similar objects: an actor.[6]

Thus some other categories adduced in this paper define these types of agents as including the following:

- Passive agents -or agent without goals
- Active agents -with simple goals
- Cognitive agents -in computer software and related electronic telecommunication these agents normally contain complex and sophisticated calculation.[7]

The agent environment can also be divided into several sub-categories which include:

- Virtual Environment
- Discrete Environment

5 Hewitt, C., "Viewing Control Structures as Patterns of Passing Messages", (1977) *Artificial Intelligence* 8(3), pp. 323-364.

6 Hewitt, C., *The foundation of artificial intelligence—a sourcebook* , Cambridge University Press. (1990), p. 147.

7 Allen, T., and Weddison R., "Can Computers Make Contracts" (1996) *Harvard Journal of Law & Technology* 26-42, p. 29.

- Continuous Environment

Agent environments can also be organized according to various properties like: accessibility (depending on if it is possible to gather complete information about the environment), determinism (if an action performed in the environment causes a definite effect), dynamics (how many entities influence the environment in the moment), discreteness (whether the number of possible actions in the environment is finite), episodicity (whether agent actions in certain time periods influence other periods), and dimensionality (whether spatial characteristics are important factors of the environment and the agent considers space in its decision making). Agent actions in the environment are typically mediated via an appropriate middleware. This middleware offers a first-class design abstraction for multi-agent systems, providing means to govern resource access and agent coordination.

3. Agents typologies: graphic representation of agents

3.1 A part view of an agent typology

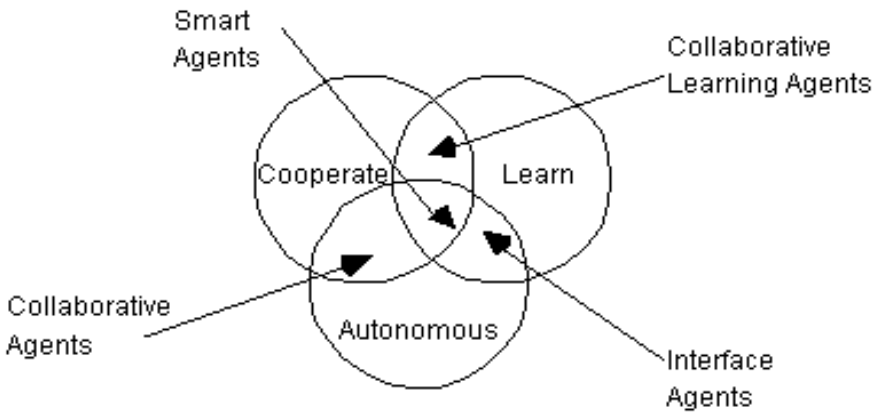


Figure 1: A Part View of an Agent Typology

These distinctions are not static, but dynamic. For example, with "collaborative agents" the emphasis is placed on cooperation and autonomy rather than on learning. But with this, it is not implied that agents never learn; it is rather just the emphasis placed on the other element of the typology. In the same vein, for the agents termed "interface agents", the emphasis is more

on autonomy and learning rather than on cooperation. But with this it does not mean anything else outside the "ë-intersecting areasi" to be an agent is considered. To put it another way, most 'expert systems' are virtually "ë-autonomous" but typically they do not cooperate or learn.

Writing back in 1993 Foner (1993: 39-40) spoke of the then existing agents as follows:

> *"... I find little justification for most of the commercial offerings that call themselves agents. Most of them tend to excessively anthropomorphize the software, and then conclude that it must be an agent because of that very anthropomorphization, while simultaneously failing to provide any sort of discourse or "social contract" between the user and the agent. Most are barely autonomous, unless a regularly-scheduled batch job counts. Many do not degrade gracefully, and therefore do not inspire enough trust to justify more than trivial delegation and its concomitant risks".*

In effect, like Foner, it is asserted here that the arguments for most commercial offerings being agents suffer from the logical fallacy of *petitio principii*- they assume what they are trying to prove - or they are circular arguments. Indeed, this applies to other ëagentsí in the literature.

In essence, *agents exist in a truly multi-dimensional space*, in which at least the following seven types of agents are identified:

There are some applications which combine agents from two or more of these categories. To these categories we refer to them as *heterogeneous agent systems*.

3.2 Classification of software agents

Figure 2: A Classification of Software Agents

3.3 Interface between electronic intelligent agents

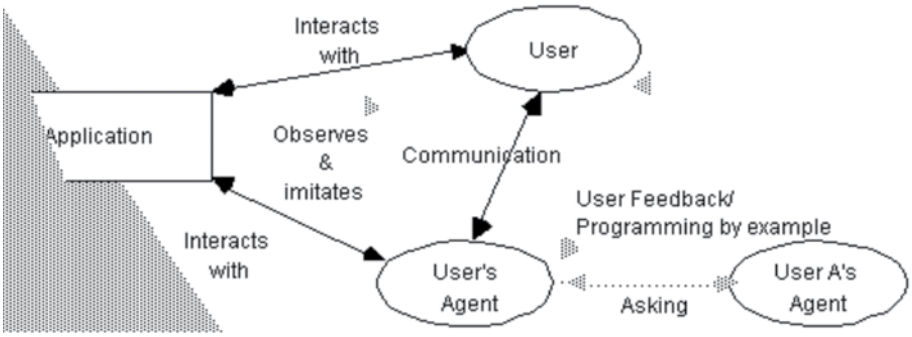


Figure 3: Interface agents

4. Legal analysis

4.1 Automated transactions= South African perspective

South African common-law principles dictate that where mistakes occur in electronic communications through the malfunction of an electronic agent, the party that installed the malfunctioning electronic agent must assume the risk of any defects or delays in the transmission. Meiring argues that the proviso in section 25(c): "…unless it is proved that the information

system did not properly execute such programming" is helpful, although not totally helpful.

Automated contract formation by means of electronic agent which is addressed in the ECT Act. The South African provisions on automated transaction were to a large extent inspired by legislative provisions in leading jurisdictions. For example, the Canadian UECA makes provision for electronic agents to conclude contracts for and on behalf of human actors, while the United States 'UETA' also provides for the legal effect of contract formation through electronic agents. Section 20 was based closely on section 10 of UETA and section 22 of the Canadian UECA.

The actions of a machine are normally attributed to the person who instructed or programmed it to perform a specific task. At common law, where mistakes occur in electronic communication through the malfunction of an electronic agent, the party that installed the malfunctioning electronic agent must assume the risk of any defects or delays in the transmission[8].

4.1.1 Legal effect of errors

As noted above, South African common-law principles dictate that where mistakes occur in electronic communications through the malfunction of an electronic agent, the party that installed the malfunctioning electronic agent must assume the risk of any defects or delays in the transmission. Meiring argues that the proviso in section 25(c): "…unless it is proved that the information system did not properly execute such programming" is helpful, but a strictly unnecessary reference to the rebuttable nature of these provisions.

However, this argument is only partly valid. The focus in addressing attribution is not on who made decisions in relation to specific transactions but on how the risk should be structured in an automated transaction. Section 25(c) of the ECT Act mitigates the risks of defects as a result of programming malfunction. Where the electronic agent merely fails to respond to a data message or where delays occur in the transmission of a data message or in the performance of an action, section 25(c) will be of little assistance. South African common law dictates that where mistakes

8 Kerr, A., Principles of a Law of Contract, 1998, pp. 110-111, Hart Publishing.

occur in electronic communications through the malfunction of an electronic agent, the party that installed the malfunctioning electronic agent must assume the risk of any defects or delays in the transmission. Section 25(c) has altered this rule as the risks associated with programming malfunction have been mitigated.

4.2 Automated transactions: Namibian perspective

To a large extent, the Namibian law on electronic transactions mirror that of South Africa. The electronic Transactions Bills based on the UN instruments on Electronic Commerce, such as the South African Electronic Communication Act is also to a large extent based on those instruments. Little research has been done on the subject in Namibia; if at all something has been researched. The Central Bank of Namibia carried out a short research on a similar subject, but on the effect of electronic commerce on the financial sector.

In contracts in general, the following elements must be satisfied for a valid contract: (1) An offer which is made by one party to another. (2) The offer must be accepted by another party. A counter-offer is a rejection of the current offer. Often the current offer is made again but there is no obligation to do so. (3) Intention to create legal relationship. This obligation is normally easy to satisfy. (4) Certainty, an ambiguous contract is void, i.e. it never existed.

Courts rarely find contracts bad for uncertainty. However, there needs to be certainty in the parties, principal undertakings, the subject matter and the price (if any) must be certain. Terms in a contract may be express or implied: For a term to be implied into an agreement it must satisfy the following requirements: (1) It must be reasonable. (2) It must be necessary to give business efficacy to the contract, so that no terms will be implied if the contract is effective without it. (3) It must be so obvious that it goes without saying.

If all these principles are applied to legal agents, some will hardly be satisfied. Obviously, the discussion is whether legal agents are 'legal personalities' is again relevant here. So far very few, if any, legal systems have attributed legal personality to "intelligent electronic agents".

In the Namibian context, several applications in the electronic environ-

ment reflect the interconnection between dependencies of several applications, which mimics the way people's activities are conducted by an organization. Dependency of intelligent electronic agents and software agents reflects an organizational form of business. In each scenario such dependency is quite different

But several common elements can be identified: Processing Dependency; 2- Simple Processing Dependency; 3- Transactional Dependency; 4- Informational Dependency.

Processing Dependency, in this form of an electronic agent operating under processing dependency, the system requires some work to be carried out remotely by other application modules in order to complete its own processing. Thus this type of "processing dependency" may fall into two sub-categories, which are (i) "simple processing dependency" where an application module needs another (probably remote) application module to perform some task before it can proceed or complete processing; (ii) "transactional dependency" where an application module requires several application modules on different, probably remote, sites to carry out some task before it can progress. In this "transactional operation mode" the operations at issue must be carried out in an 'all or nothing' fashion. Example of this transactional operation mode" is a banking transaction. Then in addition to the processing dependency, there is the "*informational dependency*". In this kind of dependency, a software application module needs to convey some information to one or more remote application modules as a consequence of some event within its jurisdiction.

5. Conclusion

In the analysis of automated transactions that employ software agents, there is still no strict rule. The rule that simply attributes the full risk to the person who installed and operates the electronic agents is too simplistic. It should be accepted with caution. Electronic agents are very diverse and interact in different environment and in different ways. Due consideration should be given to the use of multiple agents. The rule thus far encapsulated in section 25 of the South African Electronic Communication Act and by extension analogously applicable to the Namibian context, is of limited use in the context of "multiple electronic agents".

6. References

1. Foner, L. (1993), «What is an Agent, Anyway? A Sociological Case Study», *Agents Memo 93-01*, MIT Media Lab, Cambridge, MA.
2. Foner, L. (1996), "A Multi-Agent Referral System for MatchMaking", In *Proceedings the First International Conference on the Practical Application of Intelligent Agents and Multi-Agent Technology (PAAM ë96)*, London, 22-24 April, pp. 245-262.
3. Jennings, N. R. (1993), "Specification and Implementation of a Belief Desire Joint-Intention Architecture for Collaborative Problem Solving", *Journal of Intelligent and Cooperative Information Systems* 2(3), pp. 289-318.
4. Jennings, N. R., Varga, L. Z., Aarnts, R. P., Fuchs, J. and Skarek, P. (1993), "Transforming Expert Systems into a Community of Cooperating Agents", *International Journal of Engineering Applications of Artificial Intelligence* 6(4), pp. 317-331.
5. Hermens, L. and Schlimmer, J. (1993), "A Machine Learning Apprentice for the Completion of Repetitive Forms", In *Proceedings of the 9th IEEE Conference on Artificial Intelligence Applications*, Orlando, Florida: IEEE Press, pp. 164-170.
6. Kidd, D. L. and Daughertey W. H., "Adapting Contract Law to Accommodate Electronic Contracts: Overview and Suggestions" (2000) 26 *Rutgers Computer & Technology Law Journal*, pp. 215-248.
7. Garza, A. A. et al, "Monitoring and Diagnostics with Intelligent Agents– Using fazzy Logic" (007) 15 *Engineering Letters*, pp. 15-36.
8. Wooldrige M. and Jennings, N. R., "Intelligent Agents: Theory and Practice" (1995) 10 The Knowledge Enginneering.

Quasi-Property on Customer Information:Trade Secrets and Consumer Rights in the Age of Big Personal Data

by Gianclaudio Malgieri[1]

1. Introduction

In the world of Big Data[2], the intellectual capital of businesses is more and more grounded in commodification of "consumers' identities"[3]. New technologies, and in particular artificial intelligences, have extremely developed the value and potentialities of customer information for companies, especially by means of "data mining" and open data: forecasts, behaviour evaluations (based on cognitive psychology and behavioural economics)[4], studies on life expectancy, personalized marketing plan, automated profiling, creditworthiness etc.[5]

Such an intellectual work on customer information (that we can call "intellectual privacy") is highly valuable and needs specific attention. Traditionally, a trade secret is the intellectual property right used to protect these data[6]. Actually, customer information is personal data of individuals and as such, it concerns also data protection law. Moreover, data protection

1 Gianclaudio Malgieri is a Research Assistant at Sant'Anna School of Advanced Studies.

2 See O. TENE, J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. K. Tech. & Intell. Prop. 239, 2013, 257

3 N. ELKIN-KOREN & N. WEINSTOCK NETANEIL, *The Commodification of Information*, The Hague, 2002; L. LESSIG, *Privacy as Property*, 69 *Social Research, 2002,* 247-270.

4 See, e.g., J. METHA, *Economics in Competition and Consumer Policy*, University of East Anglia, ESRC Centre for Competition Policy, UEA Repository, 2013.

5 See Art. 15(1) of 95/46/EC and art. 4(3a) of the Proposed General Data Protection Regulation, which refers to "*economic situation, location, health, personal preferences, reliability or behaviour*". See F. PASQUALE, *The Black Box Society*, *The Secret Algorithms That Control Money and Information*, Cambridge, MA, 2015.

6 B. REDDIX-SMALLS, *Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market*, 12 U.C. DAVIS BUS. L.J. 87, 117-18 (2011).

rights and duties are more and more pervasive and based on a proprietary approach[7]. Therefore, "consumer identities" are the object of two intangible monopolies[8]: intellectual property of businesses and data protection rights of consumers.

In this intersection some interests are common to companies and individuals (data secrecy, reasonable measures to protect secrecy, personal data integrity, correctness of personal data), while others are controversial (right to data access, right to data portability, right "to be forgotten")[9].

Indeed, it is not just a coincidence that two parallel reforms have been proposed in the European Union in these two fields: the "General Data Protection Regulation"[10] and the first Directive on Trade Secrets[11].

In fact, in the EU the actual legal framework about the management of data management is fragmented and problematic: several member states have no trade secret protection[12], balancing rules between data protection and economic interests are quite unclear (*infra)* and the scholarly debate (in the EU and between the EU and the US) about this intersection is still at an early stage[13].

7 J.M. VICTOR, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, Yale Law Journal, 123, 2, (2013), 266.

8 Not all agree that intellectual property is a monopoly, see R. SPINELLO & M. BOTTIS, A defense of intellectual property, Edward Elgar, 2009.

9 As regards balancing interests under the Draft Data Protection Regulation see G. SARTOR, *The right to be forgotten: balancing interests in the flux of time*, Int J Law Info Tech, first published online November 25, 2015, doi: 10.1093/ijlt/eav017.

10 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011).

11 Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know- how and Business Information (Trade Secrets) against their unlawful acquisition, use and disclosure /*COM/2013/0813 final-2013/0402 (COD).

12 See, in general, BAKER & MCKENZIE, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, April 2013 (available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final- study_en.pdf).

13 See P. SCHWARTZ, D. SOLOVE, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. (2014), 877; V. MAYER-SCHONBERGER, *Be-*

In this context, several interests are in conflict and several theoretical problems require a solution. First of all, it is necessary to determine "ownership" of immaterial goods related to consumers and to understand whether allocating economic rights on personal data to consumers is efficient and consistent with the European Digital Single Market strategy[14] and respectful of personality rights of individuals[15]. Secondly, several rules in the personal data protection framework are problematic in terms of trade secrecy (right to access), competition law (right to data portability)[16], intellectual property law (right to be forgotten)[17].

In general, there is an uncertain "grey area" in which determining "default entitlement" of data is particularly challenging: it is the case of the intellectual output of customer data, all information created by (automated[18] or human) processing of raw data. In other words, it is the case of the final product of Big Data analytics and in general, all customer data which are just forecasted, statistically predicted, obtained by the original combination of probabilistic data, meta-data and raw data related to customers[19].

To find a solution to this grey area "the default entitement" issue[20], we

yond Privacy, beyond Rights-Toward a Systems Theory of Information Governance, 98 Cal. L. Rev. 2010, 1853.

14 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe* COM(2015) 192 final.

15 N. PURTOVA, *The Illusion of Personal Data as No One's Property*, Law, Innovation and Technology, vol. 7, n. 1, 2015, 83. See also D. SOLOVE, *The Digital Person*, New York, 2004, 76-80; P. SCHWARTZ, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2004, 2055; L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, N. Y., 1999, 142 ff.

16 Article 18 of Proposed General Data Protection Regulation.

17 European Data Protection Supervisor, *Opinion on the Data Protection Reform Package*, 7 March 2012, § 150- 152.

18 As regards automated creation of original databases see G. SARTOR, *Cognitive Automata and the Law: electronic contracting and the intentionality of software agents*, in Artificial intelligence and the law, 17(4), pp. 253-290, EUI Working Papers Law No. 2006/35, available at: www.ssrn.com.

19 F. PASQUALE, *The Black Box Society*, supra at n. 3.

20 This issue is even more complicated when the agents are software agents, see G. SARTOR, *Cognitive Automata and the Law*, EUI Working Papers, Law No. 2006/35, 30 and 44.

should first analyse balancing rules in the EU legal system.

Balancing rules in the EU law proves to be almost schizophrenic. In fact, on the one hand, a prevalence of trade secrets on data protection rights is proposed[21], but on the other hand, a prevalence of data protection rights on trade secrets is affirmed[22]. Moreover, in the global digital market the legal differences between the EU and the US approach to consumer personality rights[23] (and in particular to personal data protection) is a great problem in terms of international trade and the development of global economics[24].

2. Why trade secrets and not databases

The dynamism of trade secret well meets the exigencies of the "information" market[25].

Even though apparently "databases", in the form of "sui generis" probably rights related to copyright and regulated in Europe at Article 7 of 96/9/EC, are the best form of protection for collection of customer personal data, the statutory protection of "databases"[26] in Europe proves to be incomplete and inappropriate to data collection and data processing; It is difficult for companies to demonstrate specific financial investments to process such list when the processing of data is automated, the non-secrecy of the statutory protection of databases is not suitable in terms of competition strategies, the exclusive protection of the forms of expression more than of the

21 Recital 41 of 95/46/EC and Recital 51 of the Proposed General Data Protection Regulation.

22 Recital 28 of the Proposed Directive on Trade Secrets.

23 V. MAYER-SCHONBERGER, *Beyond Privacy, Beyond Rights*, supra at n. 11, 1853; P. SCHWARTZ, D. SOLOVE, *Reconciling Personal Information in the US and EU*, supra at note 11, 877.

24 E. FAHEY, D. CURTIN, *A Transatlantic Community of Law. Legal Perspectives on the Relationship between the EU and US Legal Orders*, Cambridge, 2014.

25 B.T. ATKINS, *Trading Secrets In The Information Age*, cit., 1194, which affirms that trade secret law "*is the most flexible area of intellectual property law*".

26 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, OJ 1996 L 077/20. See C. PRINS, *Property and Privacy: European Perspectives and the Commodification of our Identity*, Information Law Series, Vol. 16, 2006, 229-230.

content reveals how databases were not conceived for trade exigencies[27].

Moreover, databases tend to consider data as "units", atoms, concretely collectable in a static way. This view of personal data is anachronistic in the age of data driven economy: Big Data analytics, data mining, Internet of things and artificial intelligences contribute to make personal data as an "ecosystem", more than single static units[28].

To cope with this dynamic "ecosystem", the most suitable intellectual property right is trade secret, as a fluid and versatile protection of immaterial assets of businesses. In fact, trade secrets, as they protect "confidentiality", are based exactly on total secrecy, protection of the content, economic value *per se*[29].

3. The intersection of two legal frameworks

The main legislative frameworks implied in this debate are data protection laws and trade secret laws. They are both apparently "new" laws in the western legal experience, as they reflect the challenge to protect information in the new economy. However, they are also really fragmented and heterogeneous, from a supranational perspective.

After all, it is not a mere coincidence the parallel statutory revolution that affects these two subjects in the European Union. In fact, the 20-year-old European directive 95/46/EC on data protection[30] is going to be totally reformed by a General Data Protection Regulation[31], in discussion from

27 See I. LLOYD, *Legal Aspects of the Information Society*, London, 2000, 177-191. J. LIPTON, *Protecting Valuable Commercial Information in the Digital Age: Law, Policy and Practice*, 6 J. Tech. L. & Pol'y 2, 2001, §1; P. DAL POGGETTO, *La protezione giuridica delle banche dati mediante il diritto d'autore ed il diritto sui generis,* in Informatica e diritto, 1997, 159.

28 N. PURTOVA, *The Illusion of Personal Data as No One's Property* , 2015, supra at note 13.

29 P. SAMUELSON, *Information as Property: Do Ruckelshaus And Carpenter Signal A Changing Direction In Intellectual Property Law?*, 1989 Cath.U.L. Rev., 365.

30 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23/11/1995, 31-50.

31 European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of indi-

2012 by the European institutions. At the same time, the European Union for the first time is going to approve a directive on trade secrets[32], a subject before left to the single national laws[33].

It is clear that this strong exigency to harmonize and centralize (as regards data protection from a directive to a regulation; as regards trade secrets from heterogeneous national laws to a directive) derives from the fluidity of "data economy" in the global digital world and stimulates a comparison with the main interlocutor of the global trade: the United States[34].

Unlike European law, the US law on trade secrets is already "centralized" since 1979 by the Uniform Trade Secret Act[35]. The Act allows each state to implement it with a national law, and so the effect would be very similar to the proposed European directive: a common base with different laws reflecting each territorial industrial peculiarity[36].

At the same time, unlike European law, the US law on data protection is neither uniform, nor divided in national statutes, but fragmented per area and based on self-regulation. This situation has stimulated scholars and case law to use trade secret law to try to better protect customer databases, and this is very interesting for our purposes[37].

viduals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

32 Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against their unlawful acquisition, use and disclosure /* COM/2013/0813 final - 2013/0402 (COD).

33 See, in general, BAKER & MCKENZIE, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, April 2013 (available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf).

34 See Proposal for a Directive on the Protection of Undisclosed Know-how and Business Information, cit., Explanatory Memorandum, Context of the Proposal, §1.

35 Uniform Trade Secrets Act (UTSA), published by the Uniform Law Commission (ULC) in 1979 and amended in 1985.

36 See B.T. ATKINS, *Trading Secrets in the Information Age*, cit., 1195.

37 S.K. SANDEEN, *Relative Privacy: What Privacy Advocates Can Learn From Trade Secret Law,* 2006 MICH. ST. L. REV. 667; J. McNEALY, *Who Owns Your Friends? Phonedog v. Kravitz and Business Claims of Trade Secret in Social Media Information*, 39 Rutgers Computer & Tech. L.J. 30, [2013].

However, this issue is likely to be analyzed from an inter-institutional perspective: the proximity to the concept of "property", the relevance of human rights at issue and the social dangerousness of information espionage require the parallel intervention of civil law and criminal law[38].

4. Risks and damages: the dimension of the problem

The importance for legal science to address these issues is revealed by the incredible growth of unfair practices aiming at misappropriating trade secrets, such as theft, unauthorized copying, economic espionage, breach of confidentiality requirements. A phenomenon obviously amplified by globalisation, longer supply chains, increased use of information and communication technology[39].

Just to understand the dimension of the problem, it is useful to quote some figures: according to unofficial estimates of the US Defense Department, the industrial espionage and misappropriation of intellectual property and sensitive data cause damages of about a trillion dollars a year[40]. Furthermore, the International Center for Strategic Studies in Washington estimated that cybercrime and cyber espionage cost the US economy 100 billion dollars a year, and the global economy about 300 billion dollars[41]. From 2011 to 2014 cyber-espionage has registered an increase of 146% in the world[42] and, for example, an increase of 200% in Italy[43].

Regarding data breaches, over 22,960,000 cases of data breaches involving personally identifiable information were reported in the US through July of 2011, and in 2009 through 2010, over 230,900,000 cases of personal data breaches were reported[44]. What is even more interesting is that the 22% (the second biggest cause) of data breaches confirmed around the

38 See Proposal for a Directive on Trade Secrets, cit., Impact Assessement, § 2.2.

39 See Proposal for a Directive on Trade Secrets, cit, recital (3).

40 P. PASSERI, Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level, UNICRI, 2014, 52.

41 Ibidem, 53.

42 Ibidem, 49.

43 See CLUISIT, *Rapporto Cluisit 2015 sulla sicurezza ICT in Italia*, Milan, 2015.

44 Sec. 2 (11), S.1995 - *Personal Data Protection and Breach Accountability Act* of 2014.

world were perpetrated by cyber-espionage[45], so revealing the strong link between personal data protection and trade secrets protection.

5. Theoretical implications

This technical debate implies even a bigger theoretic revaluation of the "information" as a good, also considering all implications on competition law, intellectual property and data protection law[46].

However, our issue reveals the necessity to renew some traditional legal categories: the concept of "secret" may revolutionize the traditional legal approach to the "information" good[47]. The blurred difference between "secrecy" and "privacy"[48] involves the difference between information property (or quasi-property[49]0 and personal human rights[50].

Two opposite options may solve this theoretical conflict: the "commodification" of personal data[51] or the reconsideration of "personality" of legal persons. A compromise between these two extremes would be necessary to cope with this challenge: the overcoming of traditional barriers and a

45 Verizon Enterprise, *2014 Data Breach Investigations Report,* Executive Summary, 3 (available at http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf).

46 In the US the precise collocation of "trade secret law" has implied several problems. Modern trade secret law has been described "*as a combination of contract, tort, agency, trust, and equity law supplementing the common-law right of invention*". B.T. ATKINS, *Trading Secrets In The Information Age: Can Trade Secret Law Survive The Internet?*, 1996 U. Ill. L. Rev. 1151; See also A.H. SEIDEL, *What the General Practitioner Should Know About Trade Secrets And Employment Agreements*, 2d Ed., Philadephia, 1984, § 1.01.

47 See P. SAMUELSON, *Information as Property: cit.*, 365, where only trade secrets are considered "property" (though immaterial) because of the role of "secrecy" on information.

48 See *infra,* Section 1, final § 4.

49 D.G. BAIRD, *Common Law Intellectual Property and the Legacy of International News Service v. Associated Press, 50* U. Chi. L. Rev. *411 (1983); ID., Misappropriation, and Preemption: Constitutional and Statutory Limits of State Law Protection,* 1983 Sup. Ct. Rev. 509.

50 See P. SAMUELSON, *Information as Property, cit.*

51 N. ELKIN-KOREN & N. WEINSTOCK NETANEIL, *The Commodification of Information*, The HAGUE, 2002; L. LESSIG, *Privacy as Property*, 69 *Social Research* 247-270 (2002).

complex shared management of secret data.

6. Definition and requirement of trade secret… in the Information Age

What is the right meaning of "trade secrets" and of "personal data" in our legislative framework? Many expressions are used to generically define "trade secrets": confidential documents, secret information, commercial secrets, sensitive economic data, protected contents, e.tc.[52]. In the global Information Society it is extremely important to have clear definitions of trade secrets.

In Europe, each jurisdiction has adopted heterogeneous eligibility standards for information to be qualified as trade secrets[53]. In fact, as the Explanatory Memorandum of the Proposal for a Directive reveals, "trade secret-based competitive advantages are at risk (reduced competitiveness): the fragmented legal protection within the EU does not guarantee a comparable scope of protection and level of redress within the Internal Market"[54].

Unfortunately, in the matter of data secrets, international agreements are vague and general, as this subject is considered really susceptible to industrial and economic differences between countries, and so, a "minimum approach" has been preferred[55].

The first and unique international definition of trade secrets comes from the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPs Agreement). Article 39, section 2, in fact, defines trade secrets as "information [that] is secret, in the sense that it is not (…) generally known

52 P. WACHSMANN, *Le droit au secret de la vie privée*, in F. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l' homme*, Bruylant, 2005, p. 120.

53 BAKER & MCKENZIE, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, April 2013 (available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf), p.4-5.

54 Proposed Directive on Trade Secret, supra, *Explanatory Memorandum*, §2.2.

55 See, similarly, why in the USA the resulation of trade secrets was addressed at state level, Trading secret, 1195. See also, in general, C.R.J. PACE, *The Case for a Federal Trade Secret Act*, 8 Harv.Jour. Law & Thech., 427 (1995).

among or readily accessible to persons within the circles that normally deal with the kind of information in question; [that] has commercial value because it is secret and has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret".

In Europe, despite the above heterogeneity, a common core of requirements for trade secrets among member state laws can be found in: a) technical or commercial value of the information related to the business; b) secrecy in the sense of a not general notoriety or easy accessibility; c) economic value consisting of conferring a competitive advantage to its owner; and d) reasonable steps taken to keep it secret[56].

As regards the Proposed European Directive on trade secrets, it defines at Article 2, paragraph 1 the meaning of "trade secret", which is the exact reproduction of Article 39(2) TRIPs, with its lack of detail. For example if the requirement of "reasonable steps to protect secrecy", as vague as it is, can be appropriate in an international agreement, it shows an unacceptable degree of detail in a European framework of harmonization[57].

The probable result will be presumably that each member state will implement a different "trade secret" eligibility test on confidential information[58], with the risk that some information will be totally protected in some parts of EU and will be unprotected in some other parts. The information which most risks to suffer this heterogeneity is customer data, which traditionally are not unanimously considered fulfilling trade secret requirements[59].

An interesting model that should be considered with respect to this issue is US law. The US is the major trading partner of Europe, and also, has a long tradition in establishing legal rules protecting trade secrets, and has

56 BAKER & MCKENZIE, *Study on Trade Secrets*, supra, p. 4-5.

57 See R. KNAAK, A. KUR, R.M. HILTY, *Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for a Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against their Unlawful Acquisition, Use and Disclosure of 28 November 2013,* COM(2013) 813 Final, Munich, 2014, § 19.

58 Id.

59 See B. VAN WYK, *We're Friends, Right? Client List Misappropriation and Online Social Networking in the Workplace*, 11 Vand. J. Ent. & Tech. L. 743, 757, *passim*.

also implemented the TRIPs Agreement[60].

In the US the legal framework is clearer: the Restatement of Torts of 1939 offers six specific factors for courts to consider when determining whether a supposed trade secret is legally protectable: "(1) the extent to which the information is known outside of business (2) the extent to which it is known by employees and others involved in business (3) the extent of measures taken to guard the secrecy of the information; (4) the value of the information to the business and competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others"[61].

However, the American discipline has undergone a long development[62] which culminated in the approval of the Uniform Trade Secrets Act in 1979, emended in 1985 and now adopted by 47 of the American States. UTSA proposed a general supranational approach to trade secrets. It defines trade secrets as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy"[63].

The common denominator is undoubtedly represented by: information with competitive value (based on commercial or technical values, acquired with more or less financial investment) based on secrecy, which is actual and protected by reasonable measures.

7. When trade secrets are personal data

It is not difficult to understand the strong link between data secrets and

60 See, *WTO TRIPS Implementation*, http://www.iipa.com/trips.html (last visited April, 26th 2016).

61 Restatement of Torts 757 cmt. b (1939).

62 See, in general, S.K. SANDEEN, *Relative Privacy: What Privacy Advocates Can Learn From Trade Secret Law,* 2006 MICH. ST. L. REV. 667.

63 Unif. Trade Secrets Act 1(4), 14 U.L.A. 438 (1985).

data protection are strongly connected.

Personal data protectable under European law are defined by Article 2(a), Directive 95/46/EC[64] as "*any information relating to an identified or identifiable natural person (data subject*)" where "an identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

Commercial secrets may consist personal data[65], for instance of customers, suppliers and employees,[66] the content of negotiations with clients, the identity of those clients (customer lists), their commercial profiles, etc., are all extremely valuable elements for businesses and are all considered "confidential"[67]. In fact, customer lists are now one of the most precious assets for businesses which operate in the global market[68]: of course there are businesses for which customers' personal data are fundamental, like advertising companies, insurers, banks, etc.[69] However, in general, consumers' information constitutes a necessary intangible asset for every kind of business, because every company has clients, an advertising plan (often related to customer profiling operations), etc.[70] Actually, a great market of personal data has arisen: the so called "personal data trade"[71].

64 And by Article 4(2) of the Proposed General Data Protection Regulation.

65 Consumer data would not be personal data only if anonymized by businesses. This phenomenon is much more important with "Big Data", see in general Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, Adopted on 10 April 2014, 0829/14/EN, WP216.

66 BAKER & MCKENZIE, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, p. 5: "commercial secrets may consist of customer and supplier lists"; see also WIPO's definition "What is a trade secret", available at http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm.

67 F. MOULIERE, *Secret des affaires et vie privée*, Recueil Dalloz, 2012, p. 573.

68 See X.-T.N. NGUYEN, *Collateralizing privacy,* 78 Tul. L. Rev. *553,* [2004], which critically analyses the phenomenon of businesses, which "collateralize" customer information in secured transactions as corporate asset.

69 B. VAN WYK, *We're friends, right?,* supra, 760.

70 Ibid., 761.

71 See, *e.g.*, F. ROCHELANDET, *Economie des données personnelles et de la vie privée*, Paris, 2010, passim; A.E. LITTMANN, *The Technology Split in Customer List Interpretation*, 69 U. Chi. L. Rev. 1901, (2002), p. 1912-1914.

Taking all the above into account, the centrality of the following issues appears extremely clear. Indeed, it is necessary investigate in which terms the definitions of trade secrets can include the definition of personal information databases, and which are the conditions and restraints enabling to consider personal data of consumers as trade secrets according to the various legal frameworks of trade secret protection summarized above.

7.1 "Customer Information" in the different definitions of trade secret

In dealing with the first question, we can generally include the concept of personal data collections in the concept of valuable, secret and protected information provided for by art. 39,2 TRIPs and echoed by article 2,1(a) of the *Proposal for a trade secret directive*, although some clarifications will be necessary on the notions "secrecy" and "economic value" *(infra)*.

Recital (1) of the Proposal confirms this approach when stating that trade secrets companies tend to protect several business and research innovation management tools, which cover "*a diversified range of information, (…) such as information on customers and suppliers, business plans or market research and strategies*"[72].

Annex 21 of the impact assessment, which discusses the impact on fundamental rights, is even more explicit when it affirms: "*information kept as trade secrets (such as list of clients/customers; internal datasets containing research data or other) may include personal data*"[73].

In the USA, as well and although UTSA definition of trade secrets refers generally to "information, including (…) compilation", the Third Restatement on Unfair Competition, at chapter 4, topic 2, §39 clarifies that a trade secret "*can also relate to other*[74] *aspects of business operations such as pricing*

72 See, with the same words, Proposed Directive on Trade Secrets, cit., Memory Explanandum, §1.

73 Id., *Impact assessment*, Annex 21, 254. See, the criticisms of P. HUSTINX, *Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, Bruxelles, 12 March 2014l §11.

74 "Other" compared to "*formula, pattern, compilation of data, computer program, de-*

and marketing techniques or the identity and requirements of customers". Already the First Restatement of Torts was clear about this point. Comment "b" of section 757, clarified that "Trade secrets may be (…) a list of customers". Moreover, even if trade secret "generally relates to the production of goods (…) it may, however, relate to the sale of goods or to other operations in the business, such as a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialized customers, or a method of bookkeeping or other office management".

With reference to this difference between trade secrets related to "production" and trade secrets related to "sale", the definition in the European Proposal may be controversial. In fact, Article 2(4) defines "infringing goods" as *goods whose design, quality, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed*. Actually, it has been noted that *marketing a good* is not connected with the *use* of a trade secret. It rather constitutes a consequent act of production, but is not as such the result of a trade secret use. If the notion of "marketing benefiting from unlawful use of a trade secret" should cover also marketing campaigns based on customer lists that were unlawfully acquired, it would by far exceed the legitimate purpose of the provision if the products marketed in that manner were classified as infringing[75]. However, this issue does not contradict, and to the contrary reaffirms, the general interrelation between consumer data and trade secrets.

7.2 Conditions under which consumers' data are trade secrets… in the Information Age

However, although generically the definition of customers' personal data can be included in trade secret definition, the problem is to understand under which conditions the law protects a customer database as an intangible asset (or as an Intellectual Property right[76]) of businesses.

vice, method, technique, process, or other form or embodiment of economically valuable information (…) composition or design of a product, a method of manufacture, or the know-how necessary to perform a particular operation or service".

75 See R. KNAAK, A. KUR, R.M. HILTY, *Comments of the Max Planck Institute for Innovation and Competition*, cit., §22.

76 About the relation between Trade secrets and Intellectual Property Rights see in gen-

As in the European Union there is no uniform jurisprudence on trade secret protection, to answer this more difficult question, we can begin with analyzing how American courts have applied the 6-steps test on trade secrets to customer lists.

In other words, the test requires to determine whether a) personal information contained in the list is secret in the market and as much as possible among the employees[77]; b) the information contained in the list is of value[78]; c) the "owner" has taken "reasonable steps" or "precautions" to protect the secrecy of the list[79]; d) the "owner" has expended resources in developing the list[80] (whose information is therefore difficult to be acquired and/or duplicated)[81].

However, the diffusion of Information and Communication Technologies and the expansion of social networks over the Internet[82] complicate the application of the test. for example to secrecy of personal data, to the efforts to acquire and duplicate them and to the concrete measures of protection. Furthermore, all points enucleated above are deeply interrelated to each other: data value depends on their actual secrecy (which depends also on reasonable precautions taken) and on the efforts to acquire/duplicate those data.

a) With reference to *actual secrecy*, courts have produced some general rules to help applying the test[83]. Consumer information is secret not only if it is unavailable on public registers[84], but also on social networks "lists of friends"[85]. According to the Fifth Circuit, the general rule is that a customers' list "of readily ascertainable

eral M. PASTORE, *La tutela del segreto industrial nel sistema dei diritti di privative,* in G. RESTA, *Diritti esclusivi e nuovi beni immateriali*, Turin, 2011, 271 ss.

77 Points 1 and 2 of Restatement of torts, art. 39, 2(a) TRIPs and art. 2(1)(a) of Proposal.

78 Point 4 of Restatement, art. 39, 2(b) TRIPS, art. 2(1)(b) of Proposal.

79 Point 3 of Restatement of Torts, cit., art. 39, 2(c) TRIPs, and art. 2,1(c) of Proposal.

80 Point 5 and 6 of Restatement.

81 For the application of this test to client lists, see B. VAN WYK, *We're Friends, Right? Client List Misappropriation and Online Social Networking in the Workplace*, 11 Vand. J. Ent. & Tech. L. 743, 757.

82 *Ibid.*

83 See *Metallurgical Indus. Inc. v. Fourtek, Inc.*, 790 F.2d 1195 (5th Cir. 1986).

84 See *Infra, Section 1, § 3.*

85 B. VAN WYK, *We're Friends Right?,* 754.

names and addresses will not be protected as a trade secret"[86]. Instead, detailed information contained in a customer list, such as type and color of products purchased by the customer, dates of purchase, amounts of purchase, and certain names and addresses, are not known or available to the public[87]. What differentiate a protectable detailed client list from a non-protectable list of mere names is the large amounts of accompanying information in the list that "*could be compiled only at considerable expense*"[88].

Therefore, it is necessary that consumer information is "ancillary" beyond a simple series of names and addresses[89], but also not public on the Internet. The problem is that Social Networks contain many commercially valuable data and allow users the option of making their profiles open to the public. This free disclosure of personal data makes those data non-protectable as trade secrets: only where profiles are specifically made private, so that only contacts authorized by users to view their profiles can see them, the information in those private profiles should be considered actually secret and, thus, should be given trade secret protection[90].

86 *Zoecon Indus. v. American Stockman Tag Co.,* 713 F.2d 1174, 1179 (5th Cir. 1983); see also *Gaal v. BASF Wyandotte Corp.*, 533 S.W.2d 152, 155 (Tex. Civ. App. 1976); *Burbank Grease Servs. v. Sokolowski*, 693 N.W.2d 89 (Wis. Ct. App. 2005), review granted 700 N.W.2d 271 (Wis. 2005) (finding a list of potential customers readily ascertainable from the Internet, trade associations, and by asking customers whom to contact).

87 *Zoecon Indus.*, 713 F.2d at 1179.

88 See *Mercer v. C.A. Roberts Co*., 570 F.2d 1232 (5th Cir. 1978) (finding that a "mere list of customers," including information readily ascertainable from other sources, was not protectable as a trade secret).

89 See, e.g., *Amoco Prod. Co. v. Laird*, 622 N.E.2d 912, 918-19 (Ind. 1993) (emphasizing the importance of ease of proper acquisition in granting trade secret protection to plaintiff).

90 See I. BYRNSIDE, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 Vand. J. Ent. & Tech. L. 445, 473; *Smith v. Dravo Corp*., 203 F.2d 369, 371-72 (7th Cir. 1953) (protecting information as secret even where owner revealed the secret to others); see also *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc*., 925 F.2d 174, 176 (7th Cir. 1991) (finding actual secrecy even where thousands of drawings were in the hands of unauthorized users, in large part because of the reasonable efforts taken to maintain the secrecy of the drawings).

In this field, "privacy concerns" of users[91] allow an economic "proprietary" protection[92] of those data for businesses: the common ground is secrecy. Furthermore, this phenomenon highlights an interesting link between *privacy by design* on the Internet and reasonable precautions to protect trade secrets[93].

b) In analyzing the value of customer lists as trade secrets, a premise on the economic value of trade secret evaluation in the EU is necessary. In fact, applicable national rules do not always take into account the intangible value of trade secrets, which makes it difficult to demonstrate the actual profits lost or the unjust enrichment of the infringer where no market value can be established for the information in question. Only few Member States allow for the application of abstract rules on the calculation of damages based on the reasonable royalty or fee which could have been due had a license for the use of the trade secret existed[94].

However, US courts accepted economic value of consumer information even before Internet was such a wide phenomenon[95]. Furthermore, courts along with statutory interventions and scholarly writings[96], explicitly consider customer lists as corporate property that is both valuable and freely alienable[97]. This is confirmed also by

91 B. VAN WYK, *We're Friends Right?,* supra, 758.

92 See M. PASTORE, *La tutela del segreto industrial nel sistema dei diritti di privative,* in G. RESTA, *Diritti esclusivi e nuovi beni immateriali*, supra., P. SAMUELSON, *Privacy as Information,* supra.

93 See *infra*, Section 2, 14.1.

94 See recital (6) of the Proposal for a European Directive on Trade Secrets.

95 See e.g. *Moss, Adams & Co. v. Shilling,* 179 Cal. App. 3d 124, 129 (1986).

96 See, for e.g., *Internal Revenue Code,* 26 USC § 936(h)(3)(B)(v) (1994) (defining "intangible property" from which income can be derived as including a "customer list"). See also S.L. KROLESKI and D.R. RANT, *Use of Customer Lists: A Unified Code Is the Solution*, 15 Westchester Bus J 189, 209: "*All lists should be considered assets of the employer, as evidenced by the fact that, when a business is sold, monies are paid for such assets*".

97 For e.g., in *Miller v. Ortman*, 235 Ind 641, 136 NE2d 17 (1956), the Indiana Supreme Court held that a customer list was a part of "the good will of a business" and so freely alienable and owned by the corporation. Other more recent cases [*In re Uniservices*, 517 F2d 492 (7th Cir 1975) and *Frank v Hadesman and Frank Inc*., 83 F3d 158, 161 (7th Cir 1996)] added that the fact that the company's "customer information constitutes protectable property is underscored by the assignment thereto of independent market

several bankruptcy cases[98]. where courts focused on the correct valuation of customer lists[99].

The economic value of online contact lists is clear for many businesses, since conducting business often involves identifying the people who might be customers[100]. Depending on the particular industry, information may be more or less valuable[101].

However, it is obvious that, in the Information Society, customer (or "user") data have acquired great value. There is a wide market of personal data on the Internet[102], based on the complex intersection between marketing businesses and Internet service providers (especially Social Network Services and online stores). In fact, personal data on the web are generally called "currency" of the Information Society[103], also because their exploitation is the economic justification for the gratuitousness of most Internet services[104].

A confirmation of this "value" comes from several economic studies about privacy and digital identity: businesses can now even calculate the economic value of each digital identity[105].

---

values".

98 *In re Andrews*, 80 F3d 906 (4th Cir 1996), involved a bankrupt debtor who had sold his customer list, as part of a pre-petition sale, for approximately $1 million and the validity of the sale was not questioned. See also, *In re Lifschultz Fast Freight*, 132 F3d 339, 352 n. 12 (7th Cir 1997); *In re Roman Cleanser Co*, 802 F2d 207, 208 (6th Cir 1986) which have permitted debtors to grant security interests in customer lists, thereby acknowledging the debtors' property interest in those lists and allowing the sale of the customer lists in the normal course of business.

99 See criticisms of A.E. LITTMANN, *The Technology Split in Customer List Interpretation*, 69 U. Chi. L. Rev. 1901, (2002), 1912 ss.

100 B. VAN WYK, *We're Friends Right?,* supra, 760.

101 *Ibid.*, 761.

102 See, e.g. F. ROCHELANDET, *Economie des données personnelles et de la vie privée*, Paris, 2010, 88-114.

103 See, in general, S. LEMAN-LANGLOIS, *Privacy As Currency: Crime, Information, and Control in Cyberspace*, in *Technocrime: Technology, Crime and Social Control*, Devon, 2008, 112.

104 Trans Europe Expert, "*Le défis de la Révolution Numérique: Protection des Données Personnelles et Gratuité des Usages*", supra.

105 Boston Consulting Group, *The Value of Our Digital Identity*, Liberty Global Policy Series, 2012 *passim*, (available at http://www.libertyglobal.com/PDF/public-policy/

c) "Reasonable precautions" represent a very interesting requirement. All definitions of trade secrets require "steps"[106], "measures"[107], "efforts"[108] or "precautions" to keep information secret. However, regarding "customer information" these measures have a peculiar value because of their strong link with European data protection law. A specific paragraph will be dedicated to the comparison between "reasonable" protection of trade secret under US law and compulsory measures of protection of personal data under Article 17(1) of European directive on Data Protection and Article 30 of the Proposed Data Protection Regulation[109]. However, for the moment, it suffices to highlight that, in the European Union, there is a statutory duty to protect customer data processing by "appropriate measures", and so this trade secret requirement is always met by client lists.
d) Financial efforts to develop client lists, and the related difficulty to create or duplicate customer information represent the only requirement which is not in Article 39(2) TRIPS nor in art. 2 of the Proposal, but only in the Restatement of torts[110]. At the same time, it is the requirement which has been influenced more by the advent of the Digital Age: less resources to manage lists of data, zero efforts to duplicate and reproduce them.

Nevertheless, the "financial efforts" requirement is strongly related to actual secrecy (see point a, above) and value of secrets (see point b, above). US case law has stated that what qualifies client lists as trade secrets is the large amounts of ancillary information in the list that "*could be compiled only at considerable expense*"[111]. Moreover, (sub-b) if customer data are generally sold and bought, the "third party" business who buys customer data fulfill the requirement of financial efforts[112]. However, the work of marketing, profil-

The-Value-of-Our-Digital-Identity.pdf last visited April, 26th 2016).

106 Art. 2(1,b) of the Proposal and Art. 39, (2)(c) TRIPs.

107 Restatement of torts, sec. 757, comment b. "Definition of Trade Secret", point 3.

108 Uniform Trade Secret Act, Sec.1.(4)(ii).

109 See *Infra*, Section 2, § 14.1

110 Restatement of Torts, sec. 757, comment b, point 5.

111 See *Zeocon Indus. v. American Stockman Tag* Co., 713 F.2d 1174, 1179 (5th Cir. 1983).

112 F. ROCHELANDET, *Economie des données personnelles et de la vie privée*, supra.

ing, etc., requires many economic resources (e.g. the salary of appointed employees)[113]. Therefore, even this requirement is almost ever fulfilled.

7.3 Data protection law protects customer information even if they are not Trade Secret? The problem of "publicly available" personal information

Some personal consumer data cannot be included in the protected category of trade secrets: although requirements b) and c) are generally fulfilled[114], actual secrecy and economic resources represent a problematic point, especially in the Information Society Age[115].

Therefore, personal data which are made public on Social Network Services or which are mere lists of names do not fulfill neither the requirements of actual secrecy (*a*) nor economic resources to acquire them (d)[116]. It is now important to understand whether these "non-trade-secret" consumer data are at least protectable under European Data Protection law, otherwise we will be able to affirm a strong coincidence between protectable trade secrets and protectable personal data.

Personal data publicly available are divided in two different kinds by European data protection law: data available in public registers (e.g. administrative acts, telephone directory, etc.) and data made public by the data subject. European data protection law considers these kinds of data in four distinct cases:

1) There is a general exception to the prohibition of processing "*sensitive data*" if "the processing relates to [personal] data which are manifestly made public by the data subject" at Article 8,1(e) of directive 95/46 and Article 9,1(e) GDPS.
2) Another exception can be found with regard to the adequacy conditions of *data transfers* to non-EU countries if personal data derive

113 B. VAN WYK, *We're friends, right?*, supra.

114 See *supra*.

115 See B.T. ATKINS, *Trading secret in Information Society*, cit., A.E. LITTMANN, *The Technology Split in Customer List Interpretation*, 69 U. Chi. L. Rev. 1901, (2002), 1907.

116 B. VAN WYK, *We're friends, right?,* cit., 763.

from public registers[117]. In particular, Article 44,1(g) of the Proposal for a GDPS affirms that "*in the absence of an adequacy decision pursuant to Article 41* (decision of the Commission*) or of appropriate safeguards pursuant to Article 42* (e.g., binding corporate rules, standard data protection clauses, etc.), *a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that*: (…) *(g) the transfer is made from a register on data which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest* (…).

A similar rule can be found at Article 26,1(f) of current 46/95 data protection directive[118].

3) One last interesting exemption based on the circumstance of publicly available data has been recently proposed among the amendments of European Parliament to the Proposed General Data Protection Regulation. In particular, Article 14 provides the general obligation to inform data subject about a processing of data related to him. Paragraph (3) originally provided that if the personal data are not collected from the data subject, the controller shall also inform the data subject "from which source the personal data originate". Now paragraph (3) has been amended so that "*if personal data originate from publicly available sources, a general indication may be given*". Therefore, even if for a little scope, the fact that some data are publicly available lightens the obligations of controller (and therefore also the protection of data subject's rights).
4) Finally, Italian data protection statute (Article 24, 1(c), d.lgs. 196/2003) provides that consent is not required if the processing of

117 See R. PERRAY, "*Informatique: données à caractère personnel; formalité préalables à la mise en oevre d'un traitement de données à caractère personnel*", in *LexisNexis Juris Classeur,* fasc. 247-30, p.135.

118 For a general review about implementation of this rule under national laws, see T.J. KOBUS III, G.S. ZEBALLOS, *BakerHostetler's 2015 International Compendium of Data Privacy Laws*, on www.bakerlaw.com (available at http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf, last visited April, 26th, 2016).

personal data relates to data taken from publicly available registers or records[119].

Italian scholars have accepted a wider definition of "publicly available registers or records". In fact, it has been specified that, according to a correct interpretation of the provision, also all personal data that can be found on Internet websites can be included in the scope of Article 24, 1 (c)[120].

However, the Italian Data Protection Authority has specified that not all publicly available data can be considered in the scope of Article 24, 1(c): it has explicitly excluded, in fact, data which are public on the Internet because the reference to "registers and records" should be circumscribed to "institutional" registers only[121]. However, it has been specified that although publicly available on the Internet, personal data (in particular email addresses) cannot be indiscriminately processed[122], because it is necessary to respect the purpose for which those data were made public on the Internet. Just for the use of those data in compliance with that purpose the consent of data subject is not required[123]. However, all general principles and rules of data protection must be anyway applied to these data (except for the consent)[124].

There are no similar rules in any other European Member States, but only for example in Mexico[125] and in Canada, where paragraphs

119 Under Letter d) of the same article specifies that also data relating to economic activities that are processed in compliance with the legislation in force as applying to business and *industrial secrecy* are excepted from the consent requirement. See *infra.*

120 G. COMANDÈ, *Commento agli articoli 11 e 12 della legge 675/96,* in *La tutela dei dati personali, Commentario alla legge 675/96,* cit., 120. M.A. GARZIA, *Sub Art. 24, 1° (c),* in *La Protezione dei Dati Personali*, supra, 558.

121 Garante per la Protezione dei Dati Personali, decision 11 January 2001, in *Bollettino*, 16, 39.

122 Garante per la Protezione dei Dati Personali, Decision of 28 May 2002, Bagnara c. Consulenza Imm. Maggio; Decision of 29 May 2003, in *Relazione del Garante per la Protezione dei Dati Personali,* 2003, 91.

123 Ibid.

124 Garante per la Protezione dei Dati Personali, decision of 11 January 2001, in *Bollettino*, 16, 39. See similarly Parere Garante, 1/2000, Relazione, 2000, supra, 285.

125 Federal Law on the Protection of Personal Data held by Private Parties of July 6, 2010

> 7 (1)(*d*) and (2)(*c.1*) of Personal Information Protection and Electronic Documents Act (*PIPEDA*) provide an exception for collection and use of personal information "*without knowledge or consent*" if data are publicly available[126].

In conclusion, although European data protection law protects also "non secret" personal data, all exceptions reported above demonstrate how this protection is weaker when data are publicly known than when they are secret (regarding data transfer, sensitive information processing, and in some cases even the "consent" requirement in data processing). However, even if consumer information were not protectable as a trade secret, it would be always protected by means of "data protection" law.

The European Data Protection framework protects data subjects (and data controllers) from "personal data breach"[127], defined generally as "the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Therefore, in the European Union, even if some customer databases were not definable as trade secrets (because, *e.g.*, not totally secret), a misappropriation of them would be anyway unlawful and protected by law.

The only difference is for companies: when customer data are publicly available (e.g. in social networks) they cannot receive any intellectual property protection on their customer databases.

4. Conclusion and further stimulus: A shared quasi-property on data

How can we balance right and duties of companies in this conflict between intangible monopolies? Balancing rules in the EU framework are quite unclear and the only possible solution is an approach on a case-by-case ba-

(Ley Federal de Proteccio n de Datos Personales en Posesio n de Particulares). See, T.J. KOBUS III, G.S. ZEBALLOS, *BakerHostetler's 2015 International Compendium of Data Privacy Laws,* supra, 121.

126 For the definition and interpretation of "publicly available", see *Regulations Specifying Publicly Available Information* (SOR/2001-7).

127 See Article 17(1) of 95/46/EC directive and the explicit definition of data breach at 4 (9) of the Proposed General Data Protection Regulation.

sis[128].

The only possible solution would be a technical multi-level management of data. It would be interesting to qualify this form of cooperation in terms of joint-controlling, as the Proposed General Data Regulation encourages and better regulates this form of collaboration between individuals (data subjects) and companies (data controllers) at Article 24. This debate can offer an interesting stimulus to the issue of propertization of personal data. Several scholars, in fact, tried to define and analyze the "default entitlement" of personal data and the "de facto" property of personal data[129]. Actually, if we consider that trade secrets are considered in common law as "quasi-property rights"[130] and that the idea of quasi-property leads to a contextual right, much used to protect competition strategies[131] we can try to apply this legal concept to personal data.

Quasi-property was conceived specifically to cope with the unwillingness to "propertize" objects related to intimacy of human beings (corpse)[132] and so to cope with the unwillingness to "commodify" identity-related goods. Later, this concept developed in terms of propertization on intangible goods[133].

In conclusion, we propose to adopt a shared management of "quasi-property" on personal data, so that intellectual property rights of compa-

128 See G. MALGIERI, *Trade Secrets v. Personal Data: Possible Solution for Balancing Rights*, in International Data Privacy Law, 2016, first published online 29 January 2016.

129 N. PURTOVA, *The illusion of property,* supra at note 2013; J.M. VICTOR, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, supra at note 6.

130 S. BALGANESH, *Quasi-Property: Like, but not Quite Property, 160 U. Penn. Law Rev. 2012, 1889.*

131 Ibidem.

132 Ibidem.

133 The recent case *O' Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 112 (Ct. App. 2006) referred to "trade secrets" as "quasi-property". Also *International News Service v. Associated Press* 248 U.S. 215 (1918) referred to "information" as "quasi-property". See generally D.G. BAIRD, *Common Law Intellectual Property and the Legacy of International News Service v. Associated Press,* 50 U. Chi. L. Rev. *411 (1983) and* P.G. Baird, *Misappropriation, and Preemption: Constitutional and Statutory Limits of State Law Protection,* 1983 SUP. CT. REV. 509. See the criticisms of P. SAMUELSON, *Information as Property*, 1989 Cath. U. L. Rev., 365; C.T. GRAVES, *Trade Secret as Property: Theory and Consequences,* , 15 J. Intell. Prop. 39,2007-2008.

nies can reconcile with data protection rights of individuals, in a way both respectful of business relations both consistent with the theory of "shared privacy" and of multi-stakeholder management of the Information Society[134].

134 See M.I. COOMBS, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593 (1987); K.J. STRANDBURG, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 Rutgers L. Rev. 1235, 1298 (2005).

Does Open Data Alone Lead to Open Government?

by Aikaterini Yannoukakou[1]

1. Introduction

The inspiration for writing this paper was an article published by Eleanor Ross in the british newspaper "The Guardian" titled "Why open data doesn't mean open government"[2]. The author examines how an autocratic democracy such as China with a "…*history of cracking down on human rights activists*" decides to open all government data "…*unless it is relevant to national security and privacy*". Jonathan Gray, Director of Policy and Research at Open Knowledge Foundation, underlinesthat opening up government data does not necessarily mean that government is being democratized. Instead, it is only one –a big one indeed but still just one—step towards the democratization of a government.

Having emerged from the concept of how open data democratizes government, this paper aims to delineate the concept laying behind open data with emphasis on open government data (OGD hereafter) and the role that it is called to play in the new era of open government. The circumstances under which the releasing of data can lead to open government and which is their relation to the right to information, privacy and data protection, citizen engagement, records management and other cross cutting issues are all analysed. Also, there is a reference to how linked open government

1 Aikaterini Yannoukakou is a information scientist with a MSc from UCL, UK and currently works at the General State Archives – Historical Archives of Macedonia, Thessaloniki, Greece. She is a PhD candidate at University of Macedonia, Thessaloniki, Greece and member of the ITLaw Team.

2 The full paper is under review for the US-China Law Review Journal.

data (LOGD hereafter) can resolve the problems of access and re-use by facilitating the opening, linking, and reusing of data from heterogeneous sources.

2. Open Data

According to the Open Knowledge Foundation definition "*open means anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness)*". In other words, data is defined as "open" when it is available in any content format (text, image, sound, numbers) or software to the public without restrictions regarding its copying, further use and dissemination or its modification or its modified copies. The scale of data openness is depended by the existence or not of statutory restrictions to the above possibilities (Tsiavos, 2011).

The Open Definition gives emphasis to three very basic requirements: availability and access, re-use and redistribution, and universal participation (Dietrich, and et al., n.d.).

The emphasis is on the principle of interoperability, namely "*theability to combine different datasets together and thereby to develop more and better products and services*"(Dietrich, D., & [et.al], n.d.). The European Interoperability Framework (EIF) mentions four levels of interoperability (Hanssens, 2014, pp. 51-2):

- Technical, as referring to combining data from various sources.
- Semantic, as referring to the underlined meanings of the datasets or their metadata.
- Organizational, as referring to combining similar data sets from different sources.
- Legal, as referring to establishing the ownership of the datasets to be released.

However, an underlined question of which data should be open is still pending. It is essential –although somewhat obvious— to point out that opening up data refers only to those that does not contain personal information (i.e. birth certificates or driving licenses) or are restricted for national security and industrial espionage purposes. However, there is a thin borderline on how these licit restrictions could be used as a general

framework for restricted access and availability to otherwise perfectly postulant data for disclosure.

2.1 Why Open Data?

The importance of open data cannot be overanalyzed. It is considered as a well hidden treasure for economic growth and sustainability for the 21st century. The European Commission characterized open data as "*an engine for innovation, growth and transparent governance*" with an aggregated economic impact from applications based on open data across estimated to be €140 billion annually. focusing on three (3) primary sectors for implementation (Council COM(2011) 882):

- Untapped business and economic opportunities
- Addressing societal challenges
- Accelerating scientific progress

The report "Digital Britain 2009" describes data as "innovation currency" and "lifeblood of the knowledge economy", "*an essential raw material for a wide range of new information products and services that build on new possibilities to analyse and visualise datafrom different sources*(Council COM(2011) 882).

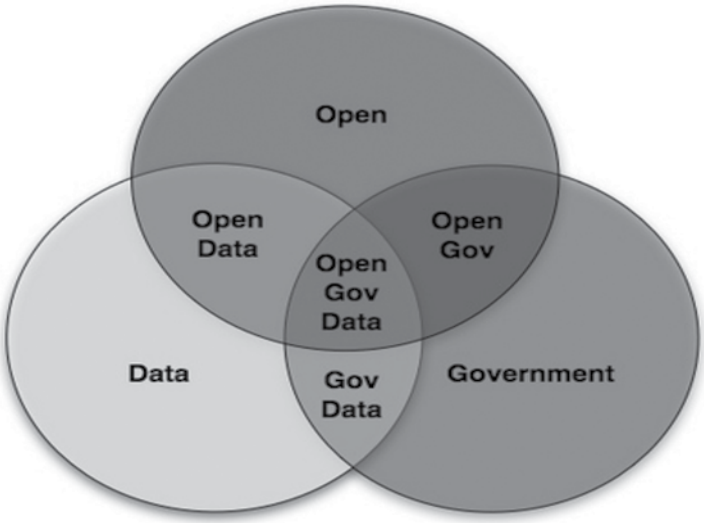
Some very illustrative examples of the economic empowerment that open data offer is market of geo-information which in German in 2007was estimated at € 1.4 billion, a 50 % increase since 2000, whereas in the Netherlands, the geo-sectoraccounted for 15.000 full time employees in 2008(Council COM(2011) 882). In the same pace, when in 2004 National Health Services in UK started to publish the outcome data for hospitals and surgeons led to reduce the mortality rates by 22% as it became easy to spot the pain points and improve cardiac healthcare services(Tinholt, 2013,p. 11).

3. Open Government Data

The term OGD refers to "*data and information produced or commissioned by public bodies or government controlled entities, which can be freely used, re-used and distributed by anyone* (Open Knowledge Foundation, n.d. ; Ac-

cess Info, 2011, p. 8). To qualify as open, government data must be able to be freely copied, shared, combined with other material, or republished as part of websites which allow users to explore, analyze, visually represent, or comment on the material, as well as transform it into other formats. Examples of the datasets held by governments which can, potentially, be opened up range from national statistics to budgetary information, from parliamentary records to data about the locations of schools, hospitals, crimes, or post boxes.

There are ten principles –eight of them released by Open Government Working Group in 2007 and two was added by The Sunlight Foundation in 2010. Data must be complete, primary, timely, accessible, machine processable, non-discriminatory, non-proprietary, license free, permanentand with reasonable usage costs.The following diagram depicts the essence and the importance of OGD by illustrating the small portion of government data that is open and the even smaller part of open data which leads to open government. Potentially the three cycles should intersect or at least be as close as to intersect with regard to data that should be excluded from publication such as personal data, national security data and industrial espionage ones or any data applying to specific protection provisions.



Picture 1: Open Government Data Venn Diagram

The Article's 19 report explicitly mentions that:

> Open data is reliant on effective freedom of information legislation. Limits on access to information and restrictions to open data should only apply if both governments and private bodies can demonstrate that making such data available would cause a specific and articulated harm to the fundamental rights of others or to society and pursue a legitimate aim. The fear of economic disadvantage does not constitute this type of harm (2013, p. 37).

3.1 Why OGD?

The three pillars of OGD are transparency, accountability and participation.Transparency and accountabilityrelate tothe obligation of governments to release data produced, collected and held by public organizations in any available form and without restrictions because they are created by the taxpayers' money. The knowledge that government information is publicly available reduces phenomena of corruption and reinforces transparency and accountability, because of a general notion that governments and public administration can be under constant scrutiny and control (Yannoukakou, 2015, p. 3257)."OGD can be used to help the public better understand what the government does and how well it performs, and to hold it accountable for wrongdoing or unachieved results" (Ubaldi, 2013, p. 4).

The participation and citizens' engagement is directly related to the possibilities offered by technology and Information & Communication Technologies (ICTs) and the advent of e-government with the creation of platforms that enable and demand the active participation of citizens in the decision-making process. Increased data transparency provides the basis for public participation and collaboration with the creation of innovative, value-added services.

A fourth dimension is the inherent potential for innovation and economic growth that OGD enclose, the so called "data economy". Open data drives growth by stimulating the creation of firms that reuse freely available government information in innovative ways.The primary objective is through the liberation and re-use of the already clustered government information to develop new products and services with added value. Each piece of information can be used numerous times from different perspec-

tives. This effectively means that government information never loses its inherent economic value, but instead awaits to be used constantly within new frameworks and combinations.For instance, the infomediary sector in Spain, a sector that comprises solely of companies that sell services on top of open data, generates 330-550 million Euros annually.The aggregate economic impact from applications based on open data across the EU27 economy is estimated to be €140 billion annually(Tinholt, 2013, pp. 8-10 ;Ubaldi, 2013, p.15). "To participate and benefit from this info- capitalist-democracy, the data subject is therefore called upon to be auditor (to monitor the granular transactions of the state in the name of accountability), entrepreneur (to make data profitable through apps and visualisations) and consumer (as the market for such apps and visualisations)" (Birchall, 2015, p. 186).

3.2 OGD considerations

The report issued by Access Info.org and Open Knowledge Foundation (OKF) in collaboration considers several technical and legal issues of OGD as binding obligations in order government data to be fully open, beneficiary to all parts involved and to lead to open government.

The technical issues focus on:

- **Discoverability:** information must be found. Releasing data online via government "data.gov" portals is not sufficient, if data is not findable.
- **Reusability:** reuse in electronic formats, machine readable and open files formats. The reusability of information depends greatly of the format of its availability. The ideal scenario is information to be released in electronic, machine readable and open file format. However, as this is not always possible, information must be available in electronic formats whenever and wherever possible, and further to update the FOIs with provisions on electronic information and to proceed to the digitization of all key information.
- **Accessibility:** regardless of the level of openness of data, information must be accessible as it increasesthe utility of the data that is released. Accessibility consists of the ability of downloading data in bulk and releasing data as rapidly and in the maximum level of detail possible following its collection.

- **Cost considerations:** the transformation of large volumes of data into reusable formats and their conversion to semantic web and linked data formats will probably encompass a severe initial potential cost implications, especially in administrations which are based on human activity for the organization and provision of information. Also, these procedures are time-consuming, especially if there is a high level of proprietary software involved, requiring a skilled ITand design team to manage them.

On the other side, the legal issues that are usually raised for the restriction of government information use refer to:

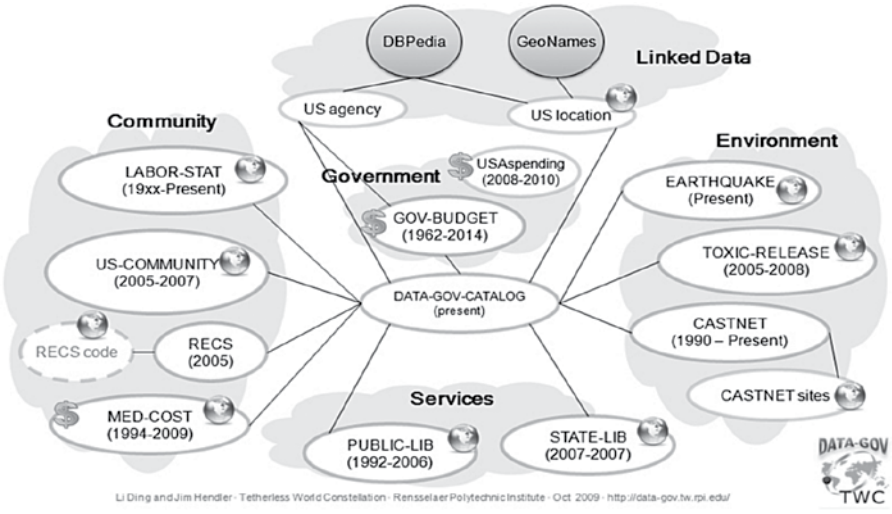
- **Legal exceptions:** the most common exceptions to public sector information release and access are the security, protection of international relationships, protection of criminal investigations, industrial espionage and privacy. However, only "protection of privacy is an internationally protected human right; the remainder are interests which may sometimes justify withholding information"(Beyond Access, 2011, p. 40).
- **Intellectual property rights:** the discussion on the copyright of public sector information is almost as old as the Berne Convention. However,the fact that information may at times be subject to intellectual property rights does not necessarily mean that it cannot be accessed and reused at all. It does mean, however, that depending on the type of license under which it is released, there may be limits on its use, or an obligation to obtain permission before reproducing or disseminating the information.(Beyond Access, 2011, p. 42).
- **Commercialization of government information:**The practice of selling data produced by public bodies to third private entities is a common practice of the economic model of government in many countries. However, it is also highly controversial due to its monopolistic point of view and because it transforms a public good to a commercial product.

Nonetheless, regardless both the technical and the legal issues involved, there are additional obstacles that are implied by the lack of standardization in re leasing OGD, namelythe various formats used, the use of different vocabularies and the quality of their accompanied metadata.

3.2 Linked Open Government Data

Interoperability and standardization are both critical dimensions when it comes to benefit from OGD in full extent. However, having interoperable and standardized OGD is not the rule. LOGD is a new linked-data web development that facilitates the opening, linking, and reusing of OGD, or putting it simply "*[LOGD]are all stored data of the public sector connected by the World Wide Web which could be made accessible in a public interest without any restrictions for usage and distribution*" (Geiger &Lucke, 2012, p. 268).

LOGD represent a new data integration paradigm for sustainable growth of OGD and consequently should be considered as the new integration application approach. Firstly, it opens up the scope of data integration from traditionally closed enterprise environments such as data warehouses to the entire Web. Users can mash up government data with crowd-sourced data, privately owned data, and many other types of non-governmental data. Secondly, it enables a data-oriented architecture (DOA) that decouples complex data objects into reusable fine-grained linked data on the Web by allowing virtually anyone to contribute LOGD deployment with partial but interlinked contributions (Ding, Peristeras&Hausenblas, 2012, p. 13).



Picture 2: LinkedData

The power of LOGD lays on the fact that it is actually a domain-independent information and data management mechanism, which penetrates various areas and domains, thus proving its advantage over traditional data management. The key concept is high-quality metadata because metadata links the data to other resources and makes the information available for re-use, and by that increasing the value of the data themselves.

4. As an epilogue

The initial question still remains.Does open data alone lead to open government?The answer to this question is a straightforward no! Open data is a technological driven movement, which focus on the use of ICTs and new technologies in order to enable the release and re-use of information under the pressure of civic society and activists on terms for the need of further transparency, accountability and participation.

However, the implementation of open government is mainly a conceptual issue. Namely, regardless whether the government information isbeing released, open and accessible, the way to open government depends on the legislative, regulatory and cultural framework of every society and its elected government. Authoritative regimes worldwide may release government data in open formats, but nonetheless it is imperative to review the type of the released data and its permissible use. Practices as censorship, extensive use of the national security and privacy exceptions, an inherent opacity and secrecy for the workings of governments only limit the scope and implementation of open government. When the regimes select and control which datasets will be released, then the release is merely a little democratic step.

Quoting Jonathan Gray:

> publishing open data is of course not sufficient for open governments or open societies. It is just one ingredient in the mix, and no replacement for other vital elements of democratic societies, like robust access to information laws, whistleblower protections and rules to protect freedom of expression, freedom of the press and freedom of assembly (Ross, 2015).

This conceptual framework comes under the umbrella of the Right to Information movement. Its theoretical approach relies on the principles of

equality, freedom for all and civil liberties as stipulated during Enlightment and were endorsed by UN General Assembly in 1948 at the Universal Declaration of Human Rights (UDHR) in which Article 19 provided for freedom of expression right as a human right and in 1966 at the International Covenant on Civil and Political Rights (ICCPR), which again in Article 19 provided for the freedom of expression right as a political right. In June 1999, the organization Article 19 published 9 principles on freedom of information legislation, which are regarded as one of the fundamental documents regarding RTI movement arguing on the universal recognition and protection of RTI as an international right. On the same page, Peled and Rabin (2011) argue on the constitutionalization of RTI anchoring their point of view to the "…its political nature and its unique role in protecting democracy" (Yannoukakou, 2015, 3254-5).

Under this notion, Geiger and Luckeunderpin that the radical change of public administration mentality relates to three concepts (2012, p. 270):

- Public and secrecy of data: everything is public, if it's not explicitly marked as secret.
- Range, type and point in time of the disclosure of data: all data, not determined by a qualified data privacy protection or data security, are fully published proactive and contemporary.
- Rights of use of the published data: published data are useable by everybody for everything including commercial usage without any restrictions exempt from charges. This includes the possibility of editing and distributing of the public data.

Probably the time has arrived for the constitutional recognition of right to information as a stand-alone right. The constitutionalization of RTI is likely to "… introduce authentic changes in state administrative procedures in addition to civil society, changes that may transform relationships between states and their citizenry" (Peled and Rabin, 2011, p. 401). The constitutional status of RTI will maximinaze all related rights along with the anchoring of the positive obligation of any State to disseminate –both reactive and proactive— government information in an equal, indiscriminatory and inclusive manner. In parallel, it will enable the creation of a solid policy framework and will enhance the international standardization of procedures regarding government data release and, thus, their exchange and re-use (Yannoukakou, 2015, p. 3260).

5. References

1. Access Info.org (2011). Beyond access: open government data & the right to (re)use public information. Available: http://www.access-info.org/documents/Access_Docs/Advancing/Beyond_Access_7_January_2011_web.pdf.
2. Article 19 (2013). Freedom of expression and ICTs: overview of international standards. Retrieved from http://www.article19.org/data/files/medialibrary/37380/FoE-and-ICTs.pdf.
3. Bauer, F., & Katlenbock, M. (2012). Linked open data: The essentials. Available: https://www.semantic-web.at/LOD-TheEssentials.pdf.
4. Birchall, C. (2015). Data.gov-in-a-box: Delimiting transparency. *European Journal of Social Theory, 18*(2), 185- 202. doi: 10.1177/1368431014555259.
5. Council Communication COM(2011) 882 final on open data: an engine for innovation, growth and transparent governance [2011].
6. Dietrich, D., & [et.al]. (n.d.). *The open data handbook*. Retrieved from http://opendatahandbook.org/guide/en/.
7. Ding, L., & Hendler, J. (2009). [Graph illustration of linked data]. *Linked Data*. Retrieved from http://www.urenio.org/wp-content/uploads/2010/12/Linked-Data.jpg.
8. Ding, L., Peristeras, V., & Hausenblas, M. (2012). Linked open government data. *Intelligent Systems 27*, 3, 11-15.
9. Geiger, C.P., & Lucke, J. (2012). Open government and (linked) (open) (government) (data). *eJournal of eDemocracy and Open Government, 4*(2), 265-278.
10. Hanssens, B. (2014).Interoperability. In *42 voices about open government*(40). Retrieved from https://www.indiegogo.com/projects/42-voices-about-open-government--43#/.
11. Mendel, T. (1999). *The public's right to know*. London: Article 19.
12. *Open Government Data Venn Diagram*(n.d.) [Graph illustration of open government data]. Retrieved from https://www.flickr.com/photos/notbrucelee/5241176871/.
13. Open Knowledge Foundation. (n.d.). Open government data Available

at: http://opengovernmentdata.org.

14. Peled, R., & Rabin, Y. (2011). The constitutional right to information. *Columbia Human Rights Law Review, 42*, 356-401.
15. Ross, E. (2015, December 2). Why open data doesn't mean open government. *The Guardian*. Retrieved from https://www.theguardian.com/media-network/2015/dec/02/china-russia-open-data-open-government.
16. Sunlight Foundation (2010). *Ten principles for opening up government information*. Retrieved from https://sunlightfoundation.com/policy/documents/ten-open-data-principles/.
17. The Founders' Constitution. Volume 1, Chapter 18, Document 35. Chicago, Ill. : The University of Chicago Press. Retrieved from http://press-pubs.uchicago.edu/founders/documents/v1ch18s35.html.
18. Tinholt, D. (2013). *The open data economy.*Retrieved from https://www.capgemini-consulting.com/resource-file-access/resource/pdf/opendata_pov_6feb.pdf.
19. Tsiavos, P. (2011). *Anoikta Dedomena kai Psifiake Sygkise (Open Data and Digital Convergence)* [PowerPoint slides]. Retrieved from http://conferences.ellak.gr/opendata2011/files/2011/12/%CE%95%CE%9B%CE%9B%CE%91%CE%9A_03_12_11PDF.pdf. In Greek.
20. Ubaldi, B. (2013). Open government data: Towards empirical analysis of open government data initiatives.In *OECD working papers on public governance* (22). Retrieved from http://dx.doi.org/10.1787/5k46bj4f03s7-en.
21. Yannoukakou, A. (2015). RTI and OGD synergy for society, economy and democracy. In Mehdi Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3254-3264). Hersey, PA: IGI Global.
22. Yu, H., & Robinson, D.G. (2012). The new ambiguity of open government. *UCLA Law Review Disclosure, 59*, 178-208.

Transitioning from the Traditional to the Electronic Medical Record: Opportunities and Ethical Considerations

by Terence N. Moyana[1]

1. Introduction

The health care field, like other professions, is witnessing major changes in information technology. One of these changes relates to the increasing adoption of the electronic medical record (EMR). The degree to which the EMR has been incorporated into medical practice relates to a number of factors such as affordability, the structure of the health care system in a particular jurisdiction, and privacy and ethical issues (Hannan, 1996; Ludwick, 2009). Due to these factors, the net result is that there are still jurisdictions where the main instrument of record-keeping is paper-based, henceforth referred to as the traditional medical record (TMR) because going back in time, most patient records took this form (Hannan, 1996; Boonstra, 2010). However, others have made major strides in implementing the EMR. Herein, we review the factors that have been the impetus in the transformation from the TMR to the EMR and the concominant ethical issues.

2. The traditional medical record

2.1 Paper-based record

The TMR generally refers to a paper-based record. It takes the form of a chart or file that is kept with the patient by the bedside or in the room/unit. Health care personnel such as doctors, nurses, pharmacists, physiotherapists and technologists enter their findings, investigations, progress notes and orders therein. As such, the TMR is the main means of communication. The physical proximity of the TMR psychologically provides a sense of security as to privacy and confidentiality (Boonstra, 2010; Manojlovich, 2015). However, it is not uncommon for patients to be wheeled

1 Full Professor, Department of Pathology and Laboratory Medicine, Faculty of Medicine, University of Ottawa.

from one part of the hospital to another, as for example, to the medical imaging department, surgical operating rooms or the intensive care unit. In these instances, the TMR usually goes with the patient, and there is greater potential for loss of privacy in the process. In addition, clinicians may take the chart to their office or other space to complete documents, and this can provide an access gap for other clinicians during that time.

2.2 Department of health records

Upon discharge from hospital, the TMR usually gets transferred to the health records department of the hospital. Since most of the large hospitals have hundreds of beds, during the course of a year a voluminous amount of TMRs is generated. This creates space and storage pressures which to a limited extent can be alleviated by techniques such as microfilming. However, ultimately other solutions have to come into play, for example, storage in lesser utilized areas of the hospital (e.g. hospital basements) but nonetheless these areas have to meet certain workplace safety standards. In other instances, the records have to be shipped off-site to places under hospital management or as part of private/public partnerships. In addition, some of the departments that contribute to the TMR (for example medical imaging, pathology and laboratory medicine, pharmacy) keep copies of their own reports so that they can cross-reference to previous reports. Annually each of these departments produces thousands of reports which at year-end are filed in binders based on accession numbers and/or in alphabetically order. This creates storage and environmental issues.

2.3 Portability of information

The issues with the TMR get exarcebated as communities get larger. With big cities, people frequently live in one community and travel considerable distances to work. As such, they may be in different places during the week and on weekends. Since the paper chart can be read by only one person at a time who needs to possess it, portability of information may be problematic, and could lead to a situation where there is more than one version of the medical record (Hannan, 1996; O'Malley, 2010). A similar situation may pertain to patients who get transferred from one hospital to another, or to nursing home or cancer centre.

3. Electronic medical record (EMR)

3.1 The transition

There are a number of barriers to be overcome in transitioning from a TMR to an EMR. For example, in the TMR, reports are handwritten or dictated and forwarded to the transcriptionist for typing, then edited and entered into the medical record for permanence. The simplicity and autonomy that is offered by this model holds much appeal particularly for solo physician practitioners or small group practices (Manojlovich, 2015). Furthermore, staying with the TMR removes the concerns about new equipment costs, learning curves, proprietorship and interoperability issues associated with the EMR (Boonstra, 2010).

3.2 Evolution to the EMR

The evolution to the EMR started with tertiary care medical centres. These tend to be big hospitals, with 500 beds or more. They have enough volume to justify the costs involved in hiring personnel and purchasing equipment (Boonstra, 2010). These hospitals generally have a high degree of specialization and the complexity of care requires large teams of people to work together. The EMR acts as a tool for enhancing communication and coordinating care. It allows the broader health care team to see data electronically in real-time which greatly reduced latency and increases turnaround time. This provides more synchronized and integrated care and thus reduces errors (Boonstra, 2010; Flegel, 2008). Paper tools are unable to deliver this level of complexity. Concurrent advances in and increased utilization of voice-recognition systems instead of transcriptionists have further enhanced the role of the EMR. Electronic records can also be organized in different formats to meet individual needs and are amenable to data indexing which makes it easier to find information (Hannan, 1996; Manojlovich, 2015).

3.3 Organization of the EMR in a hospital setting

Each department can be organized in such a way that it has its own information system where reports are generated (best of breed systems approach). As soon as the report is completed, it is verified, and at this point

becomes available to the hospital-wide EMR for the larger health care team. Such a set-up allows various units or departments such as medical imaging, nuclear medicine, pathology and laboratory medicine to customize reports according to their databases (e.g. incorporation of images in the database, synoptic reports instead of free-texting, canned texts, and report format) but at the same time maintain cross-connectivity to the central EMR (Park). Thus, data interoperability is an important aspect, and can be facilitated by making it a precondition for certification of EMR vendors in the jurisdiction. Furthermore, exchange of information can be made easier by adoption of core standardized terminology, for example, in the classification of diseases, medical procedures, services, and drugs (Boonstra, 2010; Flegel, 2008; Manojlovich, 2015). Discrete data is more amenable to data sorting and analysis.

3.4 Data entry and access

An important component of the EMR is data entry and access. Every patient, in addition to general demographic information, is assigned a health number, medical registration number and departmental accession number. These numbers can be used for bar-coding to facilitate electronic identification of the patient's records. These procedures significantly minimize the risk of record mix-ups compared to manual methods. Each person who is granted log-on privileges is required to sign into the system and undertake to maintain and respect privacy and confidentiality every time he/she logs in. There is a robust monitoring system with tracking capabilities. This means that once a report has been verified and appears on the main EMR, it assumes permanence. It cannot be changed without proper documentation and tracking; as such, it is amenable to discovery. There is a glossary of terms that can be used to indicate how the original of document has been altered. Terms such as addendum, revised, corrected or amended report can be used depending on the jurisdiction and the manner in which these terms are defined (Babwah, 2014).

3.5 Regionalization

Another factor driving the adoption of the EMR is the phenomenon of regionalization. This is a process whereby a number of small, medium and

large health care centres and hospitals in a particular region consolidate services so that they are functionally integrated, the so-called hub-and-spoke model (Fung-Kee-Fung, 2014). This streamlines administration and simplifies decision-making, creates economies of scale through centralized planning of human resources and equipment purchasing, and eliminates reduplication. For example, instead of having magnetic resonance imaging and technologists at every clinic or health centre, these facilities can be centralized to the larger hospitals and regional access can be facilitated through the EMR by using electronic referral (e-referral) and e-booking. The system can also be used for e-consulting and e-booking.

4. Ethical issues

4.1 Patient autonomy, privacy exposure and risk

Once regionalization of the various hospitals takes place, the process of e-connectivity, through incentivization, can be extended to smaller settings and even to individual practitioners such as family physicians and pharmacists. Regions can in turn be linked to other regions in the province/state or country. Indeed, in those jurisdictions with a dominant single-payer system such as Canada, this simplifies the process of patient information-sharing, e-billing, and program development e.g. analysis of resource utilization, public health, supporting research, improving quality, furthering professional education, error reduction strategies and cancer management (Murphy, 2014; Wilke, 2011). However, since these digital health networks can allow a whole range of medical systems to communicate and share information, this increases the risk that the data may be accessed by individuals not authorized to do so (Boonstra, 2010). It is a far cry from the traditional model where a patient's health was generally regarded as a matter between the individual and his/her doctor. Thus, there is an inherent tension between patient privacy and the data requirements of those agencies delivering, regulating or paying for health care (Manojlovich, 2015). Indeed, there is a tendency for institutional systems to emphasize reporting goals and broad outcomes rather than patient autonomy. Although security can be strengthened by such processes as robust log-in and tracking, and data encryption, nonetheless patients who put much value on privacy and confidentiality will feel psychologically less secure with the EMR, and

as the process continues to get rolled out and becomes systemic, this may diminish options for privacy in a publicly-funded health care system. This is particularly the case for certain conditions with a high degree of stigmatization such as drug or alcohol addiction, mental illness and developmental/genetic disorders (Sulkes, 2016). Thus, a balance has to be struck between individual rights and freedoms versus remote electronic systems that can pull massive amounts of data ostensibly for public good (Manojlovich, 2015). Ultimately, this balance should be determined by the law-makers of the land as representatives of the public. With regard to the legislative framework, there is more of a tendency to regulate the disclosure of medical information and less emphasis on placing limits on the collection of the data.

4.2 Consent

Consent for treatment has always been and will continue to be an important component of medical practice (Willison, 2003). The consent can be implied or explicit depending on the circumstances. In cases of implied consent, there is a desire to get treatment but not tie the hands of the health practitioners in such a way that it limits their ability to help the patient. For explicit consent, the emphasis is weighed more heavily on the specific instructions of the patient. The change from TMR to EMR may introduce different ways of effecting consent e.g. scanned or e-signatures. This may be to some extent a more at-arms-length procedure than the traditional signature, and may result in more automation of the process with the potential for wider dissemination of the consent within the framework on an EMR.

4.3 Individual rights versus common good

In instances of implied consent, there is the issue of downstream tests which can be automatically triggered as part of the patient's management. Once these tests are carried out, they can be accessible to third parties or discovery. A number of illustrative examples are testing for blood alcohol, HIV and genetics respectively. A person who gets involved in a motor vehicle accident may have blood collected for baseline investigations and transfusion purposes but if the police get involved, they may be interested in the blood alcohol level for other reasons. Likewise, for conditions such as HIV

or other infectious diseases which may come into the differential diagnosis, the rights of the individual for privacy have to be balanced against rights of family members and/or public good. Similarly, there may be certain conditions that may not apparent on admission into hospital but become suspect during the course of the illness and may necessitate genetic testing. The results may have implications for family members, insurance companies and employment prospects. In all these instances, the rights of the patient have to be weighed against public good or special interests. The laws governing these issues vary from jurisdiction to jurisdiction but it is clearly important to know the meaning of consent in such cases.

4.4 Secondary use of the EMR

Patients generally agree with the idea of the EMR being used as a tool for coordinating and enhancing their care. There is also the use of the EMR information for secondary purposes, for example, for public health campaigns (e.g. immunization, disease outbreaks, cancer prevention), immigration, insurance companies, and advertising (Perera, 2011; Stiles, 2011). In these situations, it can be difficult to safeguard the patient's interest due to cost containment. The current status in most jurisdictions is that this is acceptable provided certain safeguards. However, there can be a conflict between ethics and business-driven imperatives. In line with this, most institutions now have an ethics board whose function is amongst others to promote best practice.

5. Conclusion

Advances in information/electronic technology have changed the practice of virtually all professions, medicine included, in an irrevocable way. The enhancement of communication offered by electronic communication, the synchronization of care and the complexity of modern medicine make it virtually impossible to go back to paper tools. At the same time, the capacity for scrutiny increases and with this comes greater privacy exposure. This requires organizations to proactively promote a culture of respect for patient privacy and individual rights and freedoms but this has to be counterbalanced by public good as promulgated by the laws of the land.

6. References

1. Babwah, Jesse Paul, Mahmoud Khalifa, and Corwyn Rowsell. «Analysis of addenda in anatomic pathology as a quality monitoring initiative.» *Archives of Pathology and Laboratory Medicine* 138.11 (2014): 1514-1519.
2. Boonstra, Albert, and Manda Broekhuis. «Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions.» *BMC health services research* 10.1 (2010): 1.
3. Flegel, Ken. «Getting to the electronic medical record.» *Canadian Medical Association Journal* 178.5 (2008): 531-531.
4. Fung-Kee-Fung, M., et al. «Piloting a regional collaborative in cancer surgery using a "community of practice" model.» *Current Oncology* 21.1 (2013): 27-34.
5. Hannan, Terry J. «Electronic medical records.» *Health informatics: An overview* (1996): 133-148.
6. Ludwick, Dave A., and John Doucette. «Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries.» *International journal of medical informatics* 78.1 (2009): 22-31.
7. Manojlovich, Milisa, et al. «The Effect of Health Information Technology on Health Care Provider Communication: A Mixed-Method Protocol.» *JMIR research protocols* 4.2 (2015).
8. Murphy, Daniel R., et al. «Electronic health record-based triggers to detect potential delays in cancer diagnosis.» *BMJ quality & safety* 23.1 (2014): 8-16.
9. O'Malley, Ann S., et al. «Are electronic medical records helpful for care coordination? Experiences of physician practices." *Journal of general internal medicine* 25.3 (2010): 177-185.
10. Park, Seung L., Anil V. Parwani, and Liron Pantanowitz. «Electronic Medical Records.» *Practical Informatics for Cytopathology*. Springer New York, 2014. 121-127.
11. Perera, Gihan, et al. «Views on health information sharing and privacy from primary care practices using electronic medical records.» *Interna-*

tional journal of medical informatics 80.2 (2011): 94-101.

12. Stiles, Paul G., et al. «Ethically Using Administrative Data in Research Medicaid Administrators' Current Practices and Best Practice Recommendations.» *Administration & Society* 43.2 (2011): 171-192.
13. Sulkes, Stephen B. «Electronic Medical Records.» *Health Care for People with Intellectual and Developmental Disabilities across the Lifespan*. Springer International Publishing, 2016. 335-343.
14. Wilke, R. A., et al. «The emerging role of electronic medical records in pharmacogenomics.» *Clinical Pharmacology & Therapeutics* 89.3 (2011): 379-386.
15. Willison, Donald J., et al. «Patients' consent preferences for research uses of information in electronic medical records: interview and survey data.» *Bmj*326.7385 (2003): 373.

The Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria

by Nneka Obiamaka Umejiaku[1] & Mercy Ifeyinwa Anyaegbu[2]

1. Introduction

The need to combine ethics and law in regulating the activities of cyber world cannot be overemphasized. This is crucial in order to curb the menace of cybercrime which has eaten deep into the fabrics of the society. Information technology has made the world a global village and has enhanced every sphere and sector of the society like economy, commerce, social and educational sectors. Despite the advantages, the society is threatened by the growing trend of cybercrime. Arguably, cybercrime thrives because of lack of universal legal framework and jurisdictional challenges that make it difficult to bring cyber criminals to justice. For example, someone could be in Nigeria commits a cybercrime that will have effect in South Africa and Canada respectively. The question that comes to bear is which jurisdiction is competent to try him, will he be held accoutable by South African law or Nigeria law. This challenge has exacerbated the criminal activities of cybercrime in the world especially in Nigeria where it has escalated due to unemployment.

The absence of international legal Framework to combat the activities of cyber criminals has threatened the security of the State. In 2015 Nigeria

1 Lecturer, Department of Commercial and Property Law, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria, E-mail: nnekaumejiaku@gmail.com.

2 PhD, Faculty of Law Library, Nnamdi Azikiwe University, Awka, Nigeria, E-mail: ifymanyaegbu@yahoo.com.

promulgated the Cybercrime Act 2015 to curb the menace of cybercrime but the Act has failed to totally arrest the ugly trend because of some gap or lacuna and also due to so many other factors that exacerbate cybercrime in Nigeria. This work x-rays the Cybercrime Act 2015 and other legislations that have tried to combat cybercrime and also, highlights those factors that have hindered positive changes in the cyberspace.

The paper reviews the legal framework in Nigeria and observes that no law has been able to totally eradicate the menace of cybercrime. The writers are of the view that law alone is insufficient to tackle the menace of cybercrime. Due to increased technological advancement and new fraudulent devices of the cyber criminals, combined effort of both law and ethics will be a formidable tool to arrest the ugly trend and maximize the benefit of technological advancement in the information world. These efforts should not be left in the hands of the government alone. Every stakeholder in the information industry should join to win the war against and procure the security of cyberspace and its users.

2. Cyber law and ethics

The need for the regulation of the cyber world cannot be overemphasized because of the technological advancement which has transformed the world into a global village. Cyber law entails the safe and lawful collection, retention, processing, transmission and use of personal data of individuals. The need for cyber protection stems from legal models derived from a body of common rules such as the *United Nations Universal Declaration on Human Rights*[3] and the *European Convention of Human Rights* which provide for the right of every individual to privacy[4]. An instance of data protection legislation can be illustrated with the *European Convention on Human Rights* which provides for the right of respect to private and family life. It further provides that there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic wellbeing of the country? It also provides for

3 Universal Declaration on Human Right 1948.
4 European Convention on Human Rights.

the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others[5].

However, with the advances in automation of data, respective countries of the world and some national bodies like the European Union, have made a concerted effort to develop all-inclusive body of rules on data protection such as the *European Data Protection Directive and the Directive on Privacy and Electronic Communications* which incorporate principles that regulate the collection, retention, processing, transmission and use of personal data in the region.

3. Data protection principles

Under the *European Data Protection Directive, the Directive on Privacy and Electronic Communications*, and the *United Kingdom Data Protection Act*, certain principles are fundamental and they are universally agreed as "Data Protection Principles". They have formed the body of data protection laws all across major countries of the world, particularly in America and Europe. This body of principles regulates and ensures that personal data is collected, collated, processed, transmitted and transferred without infringing on the personal privacy of the individual.

These principles include the following:

- personal data shall be processed fairly and lawfully.
- personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- personal data shall be accurate and, where necessary, kept up to date.
- personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- personal data shall be processed in accordance with the rights of data

5 Ademola Adeniyi, the Need for Data Protection Law in Nigeria httpas://adeadeniyi.wordpress.com accessed on 28/10/2016.

> subject under this Act. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data should not be carried out of such countries if they do not have similar data protection laws and measures such as the European Union.[6]

4. The need for cyber law and cyber ethics

Ethics generally refers to the moral obligations that one person owes another[7]. It also refers to the standard of character set up by any race or nation[8]. Further, ethics refers to treating of morals in accordance with right principles as defined by a given system of ethics or professional conduct[9]. Cyber ethics refers to the code of responsible behavior on the Internet. Responsible behavior on the Internet in many ways aligns with acceptable behavior in everyday life, but the consequences can be significantly different.

Cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society. In the late 19th century, the invention of cameras, spurred similar ethical debates as the Internet does today. During a *Harvard Law Review* seminar in 1890, Warren and Brande is defined privacy from an ethical and moral point of view to be central to dignity and individuality and personhood. Privacy is also indispensable to a sense of autonomy, a feeling that there is an area of an individual's life that is totally under his or her control, an area that is free from outside intrusion. The deprivation of privacy can even endanger a person's health. Over 100 years later, Internet and proliferation of private data through government[10] and e-commerce is a phenomenon which requires a new round of ethical debate involving a person's privacy.

---

6 Ibid.

7 Byran A. Garner, *Black's Law Dictionary* 9th Ed., Paul Minn. 2009.

8 Albert .H. Mack Ward; the *New International Webster's Comprehensive Dictionary of the English Language*, Encyclopedic Ed., Trident Press International Florida. 2004.

9 Ibid.

10 Warren, S., Brandeis, L., "Privacy, photography and the press" *Harvard Law Review* (1998).

Cyber ethics is distinct from cyber law. Laws are formal written directives that apply to everyone, interpreted by judges and enforced by the executive power.[11] Ethics generally is the study of what is good for both the individual and society. Ethics is a broad philosophical concept that goes beyond simple right and wrong, and looks towards the good life. Information technology managers are required to establish a set of ethical standards common to their organization. There are many examples of ethical code currently published that can be tailored to fit any instrument that establishes a common ethical framework for a large group of people.

4.1 Origin of computer ethics

Computer ethics was discovered in mid-1940s by Norbert Wiener (a professor of mathematics and engineering at MIT) originally called cybernetics and include the following:

- Computer ethics deals with how computing professionals should make decisions regarding professional and social conduct.
- Who administrates the Internet?
- Internet Society (ISOC).
- Internet Engineering Task Force (IETF).
- Internet Corporation for Assigned Names and Numbers (ICANN).
- Internet Architecture Board (IAB).
- Council of Registers (CORT).
- Inter NIC.
- International Telecommunication Union (ITU).
    - Agency of United Nations that regulates ICT issues (may someday create global standards for policing the Internet)[12].

The reason for ethical use of information is not the computers but the information stored in the computers. Information ethics are the rules that define right and wrong behavior in the computing profession.

11 http://en.wikipedia.org/wiki/cyberethics.

12 Andrew Harmic, Computer Ethics and Cyber Law.

Ethics and laws are not the same. Laws are established to protect software developers (copyright and licensing) and users. Laws have penalties associated with it but ethics do not. Ethics is primarily based on principles and values. Ethics fall into three categories, the professional-which is defined by various professions (For example, lawyers have their own professional conduct or ethics which guide and regulate their activities).

- Social Ethics: This is the ethics as defined by the society in which one finds himself. There are certain moral codes or values that are already tailored by the society and the system wants one to fit into them. When one fails to adhere to these moral codes or standards, one will be regarded as social deviant or misfit.
- Individual Ethics: This is defined by personal heritage and integral values.

The need for cyber law in Nigeria cannot be over emphasized due to sudden rise of cybercrimes in the country. Recently a report indicated that Nigeria is losing about $80M dollars yearly because of software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research based in South Africa. Also the American National Fraud Information Centre reported Nigerian money offers as the fastest online scam, up to 90% in 2001[13]. The centre also ranked Nigeria cybercrime impact per capita as being exceptionally high[14]. Despite the high rate of crime in Nigeria, some scholars are of the view that cyber space should not be regulated while some assert that it should be regulated.

4.2 Regulation of the cyberspace

Cyber space has transformed the way we live in recent times. It has virtually affected every sphere of the society ranging from the economic, social, educational sector, health sector, military etc. Cyberspace has transformed the way we communicate, travel, power our homes, run our economy and obtains government services. Cyber law includes rules and regulation that

13 Mu'azu A.S., Abubakar M.K, Cybercrime in Nigeria: An overview Act 2013, *Journal of Law, Policy and Globalization*.

14 Ibid.

should be applied to curb the menace of cybercrime while ethics involve the application of moral behaviors to control the use of cyberspace. However, some authors aver that the cyber space should not be regulated offering the following reasons:

4.2.1 Freedom of expression should be an absolute right

This particular school of taught posits that regulating the Internet will grossly violate the right of privacy of individuals as provided in the *1999 Constitution of the Federal Republic of Nigeria*. Such right is absolute and cannot be qualified without irreparable damage to civil liberty in a free society. However, all rights have to be qualified in order to protect the society because absolute rights threaten other rights. For instance, unrestricted right to freedom of expression and the press on the Internet by which pornographic content exist on the Internet would threaten the right of children to be free from abuses, molestations and embarrassment. Also, fundamental rights are qualified on the basis of public policy and morality.

4.2.2 The Internet cannot be regulated because of its global nature

Another argument hinges on the fact that the Internet cannot be regulated because of its complexity. This school of thought asserts that unlike other communication network, the Internet is enormous and is not possible to regulate. However, this argument is very porous and not tenable because the cyber space remains an electronic data delivery just like other electronic communications networks such as radio, television and other telecommunications. These other networks are regulated and so should the Internet in order to secure the security of the Internet user.

4.2.3 The Internet is different in operation from other communications

It is further argued that the cyber space should not be regulated because its use is quite different from other communication network. However, this argument is untenable because its peculiar operation that requires a particular user, who seeks particular site or application, is the core reason why it should be regulated to avoid disorder or anarchy online.

4.2.4 Parental control

Another argument is that the Internet should not be regulated by the government or any organization in order to protect children from child abuse

which is perpetuated through obscene pornography on the Internet. They assert that children should be protected by their parents and not by the government.

However, even though parents, teachers and guardians and supervisors control or limit what children access on the Internet, their effort can still be supported by regulatory authorities.

5. Overview of legal framework in Nigeria to fight cybercrime

5.1 Cybercrime Act 2015

In other jurisdiction, laws that protect cyber users have existed long time ago but for Nigeria, regulation is just starting. The Act is known as the Nigeria Cybercrime Act 2015. The new Cybercrime Act signed into law on May 15, 2015 stipulates that, any crime or injury on critical national information infrastructure, sale of pre-registered SIM cards, unlawful access to computer system, cyber-terrorism, among others would be punishable under the new law[15]. The objective of the Act is generally provided as follows:

i) to provide an effective and unified legal regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

ii) to ensure the protection of critical national information on infrastructure, and

iii) to promote cyber security and the protection of computer system and networks, electronic communication data and computer programs, intellectual property and privacy rights.

Section 2 provides for its application which provides *inter alia* that the provisions of this Act shall apply throughout the Federal Republic of Nigeria. The challenge one faces with this application is the issue of geographical boundary. In the cyber space there is nothing like a geographical boundary. Delinquent youth popularly known as "Yahoo boys" have hidden under this cloak to commit serious cybercrimes. For instance somebody in Nigeria can commit a crime or dupe a company in America currency that runs

15 Joseph Onyekwere, Cybercrimes Act 2015 and need for further amendment.

in millions of dollars. The absence of international framework and cyber ethics has made the rights to privacy with regards to Internet a mirage.

To make the provision of the law real, efficient and implementable, there should be an international legal framework that will bring the culprit to justice whenever an offence is committed in cyber space.

5.1.1 Major innovations of the Act

The Act has made several innovations to ensure security of Internet users in the cyber space. The major highlights are as follows:

d) The Act provides for seven years imprisonment for all kinds of computer related fraud, computer related forgery, cyber pornography, cyber–stalking and cyber-squatting.

e) The Act criminalizes certain acts and omissions, provides best practices and provision of procedural guidelines for the investigation of such offenses.

f) The Act also defines the liability of service providers and ensures that national interest is not compromised by the use of electronic communication.

g) The Act provides a legal framework for the prohibition and punishment of electronic fraud and cybercrime whilst promoting e-government services, electronic communication and transactions between public and private bodies as well as institutions and individuals.

h) The Act gives the President the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens as constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furthermore of that. Examples of systems, which could be designated as such, include transport, communication, banking etc.

i) The Act prescribes the death penalty for an offence committed against a system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also in force against Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

j) Hackers, if found guilty, of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hacking). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

k) The Act makes provision of identity theft, with the punishment of imprisonment for a term of not less than N7 million or both fine and imprisonment. An example of identity fraud would be the individual who impersonated Chief Bola Tinubu (the former Governor of Lagos State) on Facebook and was apprehended recently by the police.

l) The Act specifically creates child pornography offences, with punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others, producing, procuring, distributing, and possession of child pornography.

m) The Act outlaws cyber-staling and Cyber-bullying and prescribes punishment ranging from a fine of not less than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.

n) The Act prohibits cyber squatting which is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than two years or fine of not less than N5 million or to both fine and imprisonment.

o) The Act forbids the distribution of racist and xenophobic material to the public through a computer system or network (e.g. Facebook and Twitter), it also prohibits the use of threats or violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to

a fine of not less than N10 million or to both fine and imprisonment.

p) The Act mandates that service providers shall keep all traffic data and subscriber information having due regard to the individual's constitutional right to privacy, and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.

q) The Act allows for the interception of electronic communication, by way of a court order by a Judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings.

The above is just an overview of some important provisions in the newly passed legislation. The Act itself contains 43 sections, and is a central piece of legislation to foster the development of the nascent ICT sector in Nigeria. Detail of this law can be found in Cybercrime (Prohibition, Prevention) Act.

5.2 Cyber protection in Nigeria 1999 Constitution

The 1999 Nigerian Constitution of the Federal Republic of Nigeria, Section 37, provides that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.[16] The individual's right to privacy is sacrosanct. It can only be fettered by laws made by democratically enabled public authorities in the interest of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or moral or for the protection of the rights and freedoms of others.[17]

i) In the interest of defense, public safety, public order, public morality or public health; or

ii) For the purpose of protecting rights and freedom of other persons surmising from the above, the right to privacy of an individual even when protected by the Constitution can be compromised by any Act

16 1999 Constitution.

17 Ibid.

of the federation which seeks to protect public safety, order and interest.

Thus, enforcement of the right of privacy, under the Nigerian constitution may not be readily obtainable; an individual may need to seek redress under other applicable laws[18].

5.3 The Economic and Financial Crime Commission Act 2004

The Economic and Financial Crime Commission Act provides the legal framework for the establishment of the Commission and protection from economic and financial crimes. Some of the major responsibilities of the Commission according to part 2 of the Act include:

a) The investigation of all financial crimes, including advanced fee fraud money laundering, counterfeiting, illegal charge, transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam among others

b) The coordination and enforcement of all laws against economic and financial crimes with a view to identifying individual, corporate bodies, or groups involved

c) The Act undertakes research and similar work with a view to determining the manifestation, extent, magnitude and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same

d) Takes charge of, supervises, controls and coordinates all the responsibilities functions and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes in consultation with the Attorney General of the Federation

e) The coordination of all investigating units for existing economic and financial crimes, in Nigeria

f) The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1994

18 Ibid.

g) The Failed Bank (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended
h) The Banks and other financial institution Act 1991, as amended, and miscellaneous offences Act.

According to section 23 of the Advanced Fee Fraud Act[19] false pretenses means representation whether deliberate or reckless, made by word, in writing or by conduct of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.

Economic crime is defined by the Act as "the non-violent criminal and illicit activity committed with the objective of earning wealth illegally, either individual or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including countering of currency, theft of intellectual property and policy open market abuse, dumping of toxic wastes and prohibited good.

This is currently the only law in Nigeria that deals with Internet crime issues and it only covers the regulation of Internet service providers and cyber cafés. It does not deal with the broad spectrum of computer misuse and cybercrimes as cited by the Criminal Code.

5.4 The Nigerian Criminal Code Act 1990

The Criminal Code Act of 1990 criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cybercrime is not mentioned in the Act, it is a type of stealing punishable under the Criminal Code. The most renowned provision of the Act in Chapter 38, deals with obtaining property by false pretenses or cheating. The specific provision relating to cybercrime is section 419, while section 418 defines

19 Advanced Fee Fraud and Related Offences Act 2006 (Source: National Assembly of Nigeria 2006).

of what constitutes an offence under the Act. Section 418 states that any representation made by words, writing or conduct of a matter of fact, either past or present, which representation is false, and which the person making it knows to be false or does not believe to be true, is a false pretence[20].

Section 419 states that any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. Despite the laudable provisions enumerated in these legal frameworks, cybercrime still thrive in Nigeria because law alone is inadequate to curb the menace of cybercrime. It is therefore recommended that these laws should be combined with ethics to totally eradicate cybercrime in Nigeria.

6. Factors that exacerbate cybercrime in Nigeria

a) Lack of Jurisdiction: The problem of jurisdiction has exacerbated the rate of cybercrime in Nigeria. The cyber criminals can sit in the confine of their room and commit a crime that will affect people in other jurisdictions. For instance, a criminal may be in Nigeria and commit an offence that will have effect in South Africa. The question will be which court will have jurisdiction to try the matter, is it the court in Nigeria or the court in South Africa? This challenge has become a stumbling block in arresting the problem of cybercrime in Nigeria.

b) Untrained Personnel/Monitoring Team: Despite the laudable provisions made by the Act, cybercrimes still thrive in Nigeria due to absence of trained personnel to prosecute the offenders. Most of the Nigerian police personnel that ought to monitor, arrest and prosecute cybercrime are not computer literate. It is therefore recommended that Nigerian police force should be subjected to constant ICT training to make them grow with the technology and be efficient and effective in their duty.

c) Lack of Job: The poverty rate in Nigeria is very high and has thrown

20 Maitanmi Olusola, Ogunlere Samson Ayinde Semiu, Adekunle Yinike.

our youths into cybercrime. Some who are graduates do not have a job and in order to survive, they indulge in cybercrime in order to make ends meet.

These youths are known as yahoo boys' and are noted for duping people.

d) Juveniles Delinquency: Juveniles are young people are under the age of eighteen. By virtue of juvenile law they enjoy protection because they are regarded as infants. The truth is that many that engage in cybercrime like phishing, spreading of computer virus, cybersquatting etc are infants that enjoy protection from the law. Thus even when they are caught, the law does not punish but rehabilitate and reintegrate them into the society because they are still malleable.
e) Lack of Implementation: The problem is not the law. The Act has made laudable provision to protect individuals and society from the menace of cybercrimes. The problem lies in implementation. The truth is that as at present, Nigeria does not have viable structures to implement the laws. The prosecutors are not trained; there are no monitoring team to oversee the activities of delinquent youth especially those that operate computer system in cybercafés.

Thus lack of implementation cripples the law and makes the right of information technology a mirage to citizens.

f) Corruption: The issue of corruption is central in many African countries. For instance, the Act provides in Sec. 32 (1) that any person who engages in computer phishing shall be liable upon conviction to three years imprisonment or fine of one million naira.

In Nigeria even when these cyber criminals are caught, the police may demand for bribe which when offered, will close the case. Corruption has enhanced the growth of Internet crime subculture. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud. Nigeria was ranked third among the most corrupt countries in the world.

g) Lack of Standards and National Central Control: Charles Emeruwa, a consultant to Nigeria Cybercrime Working Group (NCCWG), said lack of regulation standards and computer security and protection

act is hampering true e-business. Foreign Direct Investment (FDI) and foreign out sourcing are encouraging computer misuse and abuse[21].

h) Lack of National Functional Databases: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individuals records and tracing their movements[22].

i) Porous Nature of the Internet: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

j) Increased Dependency of Computer Systems: With vulnerability and dependence of computer system within global Internet. The rate of crime and damage of the new Internet technology as a result of criminal activities is significantly increasing.

k) Poor Regulation of the Internet: Cybercrime thrives on weak information protection due to poor regulation of the Internet. It is therefore imperative to give information about vulnerability of computer system due to the Internet use and necessity of effective protection means.

l) Complex Cyber Criminal Network: The emerging trend of criminal organizations working together with criminally minded technology professionals to commit cybercrime as well as fund other activities. These cyber criminal network are inherently complex bringing together individuals in real time from across the globe to commit crime on an unprecedented scale.

m) Imperfection of Domestic Legislation and Absence of International Legal Framework: Imperfection of domestic legislation and absence of International Legal Framework has greatly hiked the rate of cybercrime because great use of the Internet has significantly surpassed current national and international social and legal norm, which regulate the sphere of information protection.

21 *International Journal of Cognitive Research in Science Engineering and Education*, vol. 1, no. 1, 2013.

22 Ibid.

7. Recommendations

a) Adequate Legislation and Implementation: Cyber ethics and cyber laws are being formulated. These laws should be implemented so that the laws will be applied. International legislation should be made to avert the problem of jurisdiction which acts as catalyst in exacerbating cybercrime.

b) Training/Continuous Education: Citizens and stakeholders should be trained on the use of the Internet to be abreast with the latest trend in the cyber space in order to maneuver the schemes of cyber criminals. The police and other law enforcement agencies should undergo continuous education for effective security management.

c) Creation of Information Technology Awareness: Information Technology forums should be created to enhance the lives of the Nigerian youths so that they will not be trapped into cybercrimes.

d) Interactive Voice Response (IVR) Terminal: Technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer.[23]

e) Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient[24].

To totally arrest the menace of cybercrime in Nigeria, in line outdated and obnoxious laws must be totally overhauled to bring them *interdem* with current social and legal norm. Apart from imperfection of domestic laws, there is no precise definition and classification of cybercrime, coupled with the difficulty of interpretation and application of the regulating law enforcement agencies activities in this respect. The necessary mechanism of ensuring activities and cooperation of the law enforcement agencies for regulation of the Internet as well as proper detection and punishment of cybercrimes is not yet well developed.

23 Ibikunle Frank, Eweniyi Odunayo, *Approach to cyber security issues in Nigeria: challenges and solution*.

24 Ibid.

8. Conclusion

The recent increase in cybercrime is a major concern to the world especially with regards to e-commerce. This ugly trend has affected virtually all sectors of the society and is negatively affecting the image of the country. Nigeria is rated as one of the countries with the highest level of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country negatively to the outside world. It is therefore imperative that a combination of sound technical measures, laws and ethics are used to counter the activities of cyber criminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications. The government, stakeholders and every member of the society should exercise duty of care towards other Internet users. That is ethics, and international legal framework should be put in place to regulate the Internet; laws that cannot effectively regulate the cyber world should be jettisoned. There is also need for the government, security agencies to note that there is need to keep up with technological and security advancement.

9. References

1. Ademola Samuel Adeniyi, The Need For Data Protection Law In Nigeria. https://adeadeniyi.wordpress.com.2012/07/18,the-need-for-data-.
2. Alfreda Dudley, James Braman, Giovanni Vincent, *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices USA*, 2011.
3. Andrew Harmic, *Computer Ethics and Cyber* Law http://wikipedia.org/miki/cyberethic.
4. Cybercrime (Prohibition) Prevention Act 2015.
5. Freedom of Information Act 2011.
6. Ibikunle, F., Eweniyi, O., Approach to Cyber Security Issues in Nigeria: Challenges and Solutions*, International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE).*
7. Joseph Onyekwere, Cybercrimes Act 2015 and need for further amendments. The Guardian Newspaper, 24 August, 2015.
8. Kashmir Musa Waziri, The Legal Regime of Parents and Designs Law and its Effects on National Development. *International Journal of Hu-*

manities vol. 3, no. 2, 2011.

9. Leah McGrath Goodman,How Washington opened the floodgates to online poker dealing parents a bad hand.http://www.newsweek.com.
10. Nigerian Law Intellectual property Watch (NLIP) https://blips.com/some-basic-facts about-patent-in- Nigeria.
11. Ufuoma Barbara Akpotaire, Patent Strategies for companies Doing Business in Nigeria.http://ssrn.com/abstract=1801883.
12. Sturmer, M. (1998) Media History of Tanzania: Songea: Ndanda Mission Press.
13. The Constitution of the United Republic of Tanzania, (1977) 2005 revision Dar Es Salaam: Government Printer.
14. White, A. 'The need for the Dar es Salaam Declaration of Editorial Freedom, Independence and Responsibility', in White, A. (2012) (ed.) African Communication Research vol. 5, no. 1, pp. 5-8. Mwanza: SAUT.

The Use of Information Technology in South African Courts

By Rashri Baboolal-Frank[1]

1. Introduction

The benefits of employing fully fledged information technology in the courts of South Africa would be endless. The current status of information technology and the courts can hardly be seen in South Africa. An overview of the rues of court in relation to the encouragement of information technology is sub minimal. (Baboolal-Frank, 2015, 12) The Judge President of the constitutional court had curried support for e-filing from first world countries, however post-judicial support there has been no transformation of the court systems. This paper aims to discuss the benefits of the information technology systems adopted in the courts of first world countries and to investigate possible reasons why South Africa continues to play catch-up.

2. South Africa

The Judiciary made a statement illustrating that the Western Cape is the only province that utilised advanced information technology techniques, *inter alia* electronic filing, use of video conferencing and satellite communication for indigent witnesses in areas that are far away from the court's jurisdiction. The judiciary recognised the progression of advancements of information technology "as steps in the right direction for the utilisation of Information Technology to improve levels of efficiency" for courts (Media Statement following the Strategic Planning Session for the South African Judicial Arm of the State, 18 August 2012). These methods of employing information technology to fast track justice has been utilised and needs to become a trend instead of a noveltyin a one province project. These methods

1 University of Pretoria, Department of Procedural Law, Faculty of Law, Lynnwood Road, Hatfield, Pretoria, South Africa, email: Rashri.Baboolal@up.ac.za.

are electronic filing and record keeping, use of video conferencing and satellite communication for witnesses that are situated in distant areas, which are methods that have also curried support from the Judge President of the Constitutional Court Justice MogoengMogoeng (Baboolal-Frank, 2015).

3. UK

In 1991, recommendations were made to improve the electronic data base to three gigs of memory with a growth of memory per annum of 50 mega bytes. (Waugh, 1991, 27). Advancements in technology are relative to time as twenty five years later this amount of memory today is equivalent to little storage as our cellphones carry more memory capacity. "In the emerging 'information society', knowledge and information are treated as the core economic variables and the dominant social actors are seen as those who process information in accordance with codified bodies of knowledge" (Clark, 1997). We have developed into a society that the key to knowledge is through computers at people's fingertips, as books and knowledge can be stored in one system, and no longer in various sources of books. A quick search allows the information one needs within one's reach in minutes and sometimes even seconds.

The United Kingdom uses information technology to enhance the clerical workload of the courts such as automated summons and to ensure that the administrative work is computer generated to ease the clerical load so that justice can be more efficiently undertaken. (Clark, 1997, 14-15) Too often are the laborious workload of administration results in copious amount of time spent on administration rather on assisting people in an efficient manner.

Unfortunately, legal information technology is expensive and lies in the hands of the wealthy and few firms that can afford it.

> *The adoption of information technology in legal settings has been associated most closely with developments in the e1ite law firms where sophisticated systems are used to enhance the provision of creative and flexible legal services for corporate and institutional clients (Clark, 1997, 25).*

Technology reduces manual labour and ensures that the computer is able

to do the labour at a faster rate and more than thousand times the load. When law firms are able to produce one thousand summons a day, it is not manual labour that attends to this large quantity but computer-generated systems, speedy printers and photocopy machines. Convenience and technology go hand-in-hand as convenience is the output of advanced technology systems.

4. USA

In the United States the adoption of computerised technology in practice is to compete with other firms in relation to computers technology, to assist in relation to higher productivity (Clark, 1997, 16). The result is that information technology is employed to enhance the courts by re-engineering the structure of the court system and employing the IT professionals to ensure the system works actively and efficiently. This is a necessary measure to ensure that the computers work to their full capacity. The level of monitoring and quality of assurance of these information technology developments is a necessary measure to ensure the sustainability of the programmes to wean any glitches.

The IT professionals do the following:

> Video of Federal Judiciary Careers: Information Technology
>
> The U.S. Courts' Information Technology (IT) professionals support the courts' extensive technology programs. They make it possible for the judiciary to deliver justice in a technology-driven environment. The federal Judiciary seeks IT professionals who are in touch with the latest technology and software programs.
>
> Judiciary IT positions vary considerably depending on the position level and an individual court's needs. These professionals:
>
> - design, manage, and support computer-based information systems;
> - design, modify, and adapt software;
> - write code;
> - perform hardware maintenance and troubleshooting;
> - test and validate hardware;
> - train users in the judiciary's various technology solutions;

- demonstrate and apply their knowledge of computer processes and capabilities;
- meet with customers to help them assess their needs and identify software solutions;
- explain technical information in an understandable way to the user;
- know the capabilities, limitations, and functional applications of information technology;
- know theories, principles, practices, and usage of computer hardware and software, office database design, and data communications;
- have knowledge of Local Area Networks (LANs) and Wide Area Networks (WANs), including systems security standards;
- are familiar with operating systems, servers, and workstation products; and
- are able to work with flowcharting, form design, and control procedures.

High-level IT Managers may be responsible for entire systems and networks. In total, IT positions represent a broad range of technology duties and responsibilities. The many specialized IT positions in the courts include programmer analyst, programmer, application administrator, and network administrator.

Therefore, at the management level of the advanced electronic systems are expert IT professionals to ensure that the systems operates in accordance with its aims.

Thereafter we have litigation mechanisms used to prepare a trial such as discovery. Discovery can also be e-discovery generated through computer technology to ensure that the computers can sift to the most important information and save on hours to find the needle in the haystack buried in the paperwork. Hence '[t]he solution devised involves the appointing of an Electronic Discovery Master (EDM) to litigation cases when the amount in controversy in a federal civil case reaches a specified threshold.' This will aid the proceedings in countless ways, but most importantly, it will provide the court with the ability to once again provide justice in an efficient, effective and economical way (Parkins, 2011, 98).

Although ethical considerations have been considered throughout, a

brief additional note should be made here. If parties were as honest as they should be, an EDM system would be unnecessary, as all facts would accurately come to light in the courts of discovery. Parties would not try to hide important documents, and the expenses would be controlled by each party. However, this is clearly not the case, as the origin of electronic discovery cases is documents being deliberately destroyed or lost (Parkins, 2011, 109). Unfortunately, the American discovery process does not allow for the parties to operate in a *bona fide* manner and can maliciously bury the opposition in thousands and sometimes in hundreds of thousands of pages of paperwork before they find the documents that are most relevant to their trial.

In the USA, for the law to properly adjudicate discovery disputes it has been suggested that 'the law catches up with the technology' (Sorebo, 2009, 133) Cloud computing can be used to assist global companies in discovery of information in preparation for trial (Sorebo, 2009, 134).

In the digital age in order to progress forward, the law would have to be amended accordingly to dispose the old practices and may pave the way fornew practices, which pose challenges (Peyton, 2014, 1).

5. International Tribunals

> *Today, a host of different kinds of IT are used in the International Criminal Tribunal for the Former Yugoslavia (ICTY): video and audio recording of the court sessions; simultaneous interpretation; electronic court reporting; videoconferencing for witness hearings; and electronic files. Moreover, the ICTY maintains a web site with its decisions, background information, and sounds and images from the courtroom (Reiling, 2006, 189).*

This is the ideal situation where the proceedings are at court are electronically available and are for public knowledge through the internet, with the exception of certain cases that illicit extreme sensitivity such as cases involving minor children. It is apparent that justice can be undertaken and seen to done through information technology. Video and audio recording shows all the impressions of the witnesses to the Judge together with the expressions of the witnesses throughexamination in chief to cross exami-

nation. These videos and audio recordals also immortalise the proceedings as it will never be deleted and can be used as a frame of reference if the need arose.

6. Netherlands

In the Netherlands, the court statistics revealed the number of cases against the number of staff and types of courts the budget utilised. These figures ultimately measure the efficiency of the court and are important factors to consider when developing methods to improve the system.

> *In 2002, the judiciary had more than 8500 staff employed, a budget of E650 million and a turnover of approximately 1,583,000 cases. There are 19 district courts with normally four sectors each: a civil law sector, a criminal law sector, an administrative law sector and a local courts sector. The civil law sectors have a specialized commercial unit and a unit for summary proceedings. The formerly over 60 local courts were administratively integrated into the districts courts in 2002. They deal mostly with small money claims, traffic violations, minor family matters, and employment and rent contracts. In these fields, they also have summary proceedings. There are five appeal courts which hear appeals of civil, criminal and some administrative cases (Reiling, 2006, 190).*

So using the above variables a method was defined in order to improve the system.

> *However, how should this improvement be defined? These past years, the judiciary has been studied extensively from the perspective of organization science. This produced many significant insights on ways to enhance effectiveness and efficiency by reorganizing the courts and their processes. But organization science cannot conclusively determine how the judiciary's work of administering justice should be improved. The ultimate standard in a legal context is a legal quality standard. The most generally accepted legal quality standards are laid down in both article 14 of the International Covenant on Civil and Political Rights (ICCPR) and article 6 of the European Convention on Human Rights (ECHR): citizens are entitled to a fair hearing of their case within a reasonable time by an independent, impartial tribunal. Improved ad-*

> *ministration of justice means better compliance with the ideals in article 14 ICCPR and article 6 ECHR: fair hearing and reasonable delay. An important aspect of fair hearing is equal treatment. Citizens may reasonably expect to be treated equally when the courts ensure consistency of their decisions. We will see how courts can use IT for that purpose. Reasonable delay: Timeliness is generally considered to be a very important aspect of the services of the courts. Speedy decision-making was long held to be at odds with careful judicial consideration of cases. We will see, however, that using IT to improve consistency can actually shorten handling time as well (Reiling, 2006, 190).*

Hence the conclusion was to improve efficiency and the court systems was through information technology systems.

7. Russia

Justice Mogoeng Mogoeng supported the Russian information technology systems that were implemented, which he encouraged for a South African context. Global information technology encourages e-commerce, ultimately the veracity of digital signatures would need to be determined in the Russian context.

> *With the advent of global information technology, electronic documents are increasingly used in Russian business practice. Individual entrepreneurs and organizations enter transactions by exchanging e-mails, private users subscribe to e-mail services on the internet under contracts they sign electronically; banks introduce customer telebanking systems, and business make payments through electronic payment systems. These examples by no means exhaust the list of all potential uses of electronic documentation. In this context, it becomes necessary to determine the legal status of electronic documents in the system of Russian law (Naumov and Nikiforova 2005, p. 62).*

In Russia digital signatures are legally acceptable (Naumov and Nikiforova 2005, 62) Digital signatures are verified through certificates authenticating the signature to be verified from the digital signatory (Naumov and Nikiforova, 2005, 64).

The validation of electronic digital signatures requires not only legisla-

tion but also, an economic investment (Finocchiaro, 2002, 67).

> *Code of the Russian Federation. This provision allows the use of electronic digital signature, stating that "the use in the making of a transaction of a reproduction of a signature with the assistance of means of mechanical or other copying, electronic-digital signature, or other analogue of an actual hand-written signature is allowed in cases and by the procedure provided by a statute, other legal acts, or agreement of the parties… However, this provision suffers a number of limitations, the most important of which is that its scope of application seems limited to a transaction. Moreover, it requires an agreement or a legal provision, it does not directly apply to relations with public administrations, it does not provide to the judge criteria for a decision (Finocchiaro, 2002, 67).*

Digital signatures are not utilised all the time for commercial transaction as there are still drawbacks in using this method to conclude transactions.

8. Australia

Digital signatures in Australia are not commonly used, the electronic signatures are mainly used for online government services (Srivastava, 2009, 47).

8.1 Electronic signatures

In South Africa the Electronic Communications and Transactions Act 25 of 2002 ("the Act") deals with the legislative implications of digital signatures.

The Act deals with the veracity and validation of electronic and digital signatures.

The most important provisions of the Act are:

'advanced electronic signature' means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37;

8.2 Objects of Act

1) The objects of this Act are to enable and facilitate electronic communi-

cations and transactions in the public interest, and for that purpose to-

i) recognise the importance of the information economy for the economic and social prosperity of the Republic;

j) promote universal access primarily in underserviced areas;

k) promote understanding and, acceptance of and growth in the number of electronic transactions in the Republic;

l) remove and prevent barriers to electronic communications and transactions in the Republic;

m) promote legal certainty and confidence in respect of electronic communications and transactions;

n) promote technology neutrality in the application of legislation to electronic communications and transactions;

o) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;

p) ensure that electronic transactions in the Republic conform to the highest international standards;

q) encourage investment and innovation in respect of electronic transactions in the Republic;

r) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

s) promote the development of electronic transactions services which are responsive to the needs of users and consumers;

t) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities and, areas and the disabled are duly taken into account;

u) ensure compliance with accepted International technical standards in the provision and development of electronic communications and transactions;

v) promote the stability of electronic transactions in the Republic;

w) promote the development of human resources in the electronic transactions environment;

x) promote SMMEs within the electronic transactions environment;

y) ensure efficient use and management of the .za domain name space; and

z) ensure that the national interest of the Republic is not compromised through the use of electronic communications.

8.3 Signature

1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.
2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.
3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if-
   a) a method is used to identify the person and to indicate the person's approval of the information communicated; and
   b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.
4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.
5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that-
   a) it is in the form of a data message; or
   b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred.

(Section 13, Electronic Communications and Transactions Act 25 of 2002).

Ultimately the allowance and creation of digital signatures was to allow the conclusion of commercial transactions at the convenience of the parties. We see the conclusion of these transactions most often in the transactions dealing with the sale of a vehicle or any transaction with the banking

institutions.

In view of section 39 of the Constitution, international law in relation to consideration of the UNCITRAL model Law on electronic signatures 2001, article 2 states that:

a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval"

Electronic signatures utilise techniques such as validation through biometric devices and personal identification pins (UNCITRAL, 2001, 21).

It is apparent from the domestic legislation that electronic/digital signatures are recognised in South Africa and the legislation complements international legislation governing digital signatures.

However despite, digital signatures being used in transactions there is no use of it in legal pleadings. When we refer to the rules of court, we find that the rules do not allow for digital signatures on pleadings, which is unfortunate as it means that one attorney is confined to signing off hundreds to thousands of pleadings manually.

"Rule 18 of the High Court:

> *"Rules relating to pleading generally.- (1) A combined summons, and every other pleading except a summons, shall be signed by both an advocate and an attorney or, in the case of an attorney who, under section 4(2) of the Right of Appearance in Courts Act, 1995 (Act No.62 of 1995), has the right of appearance in the Supreme Court, only by such attorney or, if a party sues or defends personally, by that party."*

(GNR. 48 of 12 January 1965: Rules Regulating the Conduct of the Proceedings of the Several Provincial and Local Divisions of the High Court of South Africa).

In the Magistrates' Court Act, section 5(3)(a)(ii) provides for a summons to be signed by the attorney for the plaintiff or s5(3)(a)(iii) the plaintiff to sign in person if they do not have any representation.

It is apparent from the wording stipulated in the Act and rules of court, which signing electronic on pleadings are not excluded and have not seemed to be a rule of practice as it does not constitute originality on face

value. However if pleadings can be signed electronically by attorneys of the firm, it would cut the manual labour of the attorneys of signing thousands of pleadings. Perhaps an amendment to legislation regarding electronic signatures on pleadings is a necessary amendment.

9. Conclusion

The advances of information technology in the court systems are a necessary transformation for courts and justice in South Africa. Information technology creates efficiency, as it improves access to usually justice and allows the computers to generate the manual and laborious work that clerical administrators attend to. Instead, clerical administrators may assist more people to exercise their rights through assistance at court regarding suing out summons and launching applications.

Innovative technology through information technology creates necessary convenience, and ranges to digital signatures, which pleadings can be made easier, by utilising electronic signatures so that attorneys are not buried in the administration of signing thousands of summons to be issued before the court. Courts can also issue summons electronically instead of manually, which in the long term saves time and money. Information technology and the advancements are expensive but in order to make money and create time, money needs to be spent to attain an improved justice system through advancements of information technology in South Africa.

10. References

1. A. Clark, "Information Technology in Legal Services" 19 *J.L Soc'y* 13, 1992.
2. Chris Crawford at http://www.ncsc.org/Topics/Technology/Technology-in-the-Courts/Resource-Guide.aspx.
3. Electronic Communications and Transactions Act 25 of 2002.
4. G. Fiocchiaro, "The Russian Federal Law on Electronic Digital Signature as Compared to the Directive 1999/93/EC on a Community Framework for Electronic Signatures" Electronic Communication Law Review 55, 2002.
5. R. Baboolal-Frank, "Revolutionizing the Civil Courts in South Africa

Through Information Technology" OIDA *International Journal of Sustainable Development* Vol. 8 Issue 10 (2015) 11.

6. (GNR. 48 of 12 January 1965: Rules Regulating the Conduct of the Proceedings of the Several Provincial and Local Divisions of the High Court of South Africa). Magistrates' Court Act.
7. Media Statement following the Strategic Planning Session for the South African Judicial Arm of the State, 18 August 2012.
8. A. Peyton, "Kill the Dinosaurs and other Tips for Achieving Technical Competence in your Law Practice" *Richmond Journal of Law & Technology* 1, 2014.
9. V. Naumov and T. Nikiforova, "Electronic signatures in Russian Law" 2 *Digital Evidence & Elec Signature Law Review* 62, 2005.
10. Z. Parkins, "Electronic Discovery: Why the Appointment of Special Masters in All Large Electronic Discovery Disputes is Vital to the Progress of American Civil Justice" 5 *American Journal of Mediation* 97, 2011.
11. G. Sorebo, "Remote Electronic Discovery" 6 *Digital Evidence & Elec. Signature Law Review* 132, 2009.
12. A. Srivastava, "Businesses' Perception of Electronic Signatures: An Australian Study" 6 *Digital Evidence & Elec. Signature Law Review* 46 2009.
13. UNCITRAL model Law on electronic signatures with Guide to Enactment 2001.
14. P. Waugh, "The Use of Computers in the Administration of Justice in the United Kingdom" 5 *Year Book of Law Computers Technology* 26, 1991.

Artificial Reproductive Technologies and the Right to the Truth about One's Own Genetic and Biographic Origins

by Ludovica Poli[1]

1. Introduction

This paper aims at examining the right to know one's own origins arising from the application of some artificial reproductive technologies (ART). The analysis begins with a general introduction to these techniques and considers their impact on family as a social construct (2). It then ponders the double dimension of the right considered, namely the right to know one's own *genetic* origins, which appears especially relevant in the current post-genomics era (3), and the right to know one's own *biographic* origins (4). The paper proceeds considering the legal foundations of this right under international law (5.1), envisaging - in view of the case-law of the European Court of human rights (ECtHR) - possible principles to be applied in balancing it with other competing interests (5.2). It finally explains that the *conditio sine qua non* for a full exercise of the right to know one's own origins is the awareness of the means of conception, a responsibility which rests upon the recipient parents, with only a residual role for the State (6).

2. ART and the use of technology to generate children (and families)

Artificial reproductive technologies (ART) include a number of treatments involving*invitro* handling of human gametes (eggs and sperm) and embryos to establish a pregnancy.

Since the birth of the first baby resulting from *in vitro* fertilization (IVF) in 1978, ART strongly and constantly improved: nowadays techniques such

1 Assistant Professor of Public International Law, University of Turin, Department of Law.

as gamete donation, surrogacy, embryo cryopreservation[2] and embryo donation are common in many States around the world and many other improvements are certainly here to come in the near future.

Numbers reveal that this is a growing business[3], with an international dimension: many patients travel to other countries to undertake fertility treatments not available to them in their own state for a number of reasons, fueling the phenomenon of 'reproductive tourism'[4].

Aiming at generating a child, ART has a key impact on family as a social construct, only partially similar to adoption. In fact, while adoption is a legal and social instrument to create a family, ART - permitting the separation of procreation from sexual intercourse - involves a technical intervention in what has been for centuries considered exclusively a natural process. As such, ART not only permit 'the creation of families that otherwise would not exist'[5] analogously to adoption, but also offers 'alternative routes to family life, creating biological linkages that adoption bypasses'[6]. Secondly, while adoption is mainly conceived at the benefit of parentless children, ART helps adults to realize their aspiration of becoming parents[7]. More than adoption, thus, these techniques allow 'for a remarkable plu-

2 Embryo cryopreservation is the process of preserving an embryo at sub-zero temperatures, (generally at an embryogenesis stage) and it used for extra embryos. It also can be used to postpone the pregnancy for a number of reasons (of medical or different nature).

3 According to the European Society of Human Reproduction and Embryology, it is now estimated that more than 5 million babies have been born worldwide since 1978 (https://www.eshre.eu/Guidelines-and-Legal/ART-fact-sheet.aspx)

4 R.F. Storrow, *Quests for Conception: Fertility Tourists, Globalization and Feminist Legal Theory*, in *Hastings Law Journal*, vol. 57, 2005-2006, pp. 295 ss.; G. Pennings, *Reproductive tourism as moral pluralism in motion*, in *Journal of Medical Ethics*, vol. 28, 2002; pp. 337 ss.; G.K.D. Crozier, D. Martin, *How to address the ethics of reproductive travel to developing countries: a comparison of national self-sufficiency and regulated market approaches*, in *Developing World Bioethics*, vol. 12, 2012 pp. 45 ss.

5 M. Sabatello, *Are the kids all right? A child-centred approach to assisted reproductive technologies*, in *Netherlands Quarterly Human Rights*, vol. 31,2013, pp. 74-75.

6 E. Waldman, *What do we tell the children?* in *Capital University Law Review*, vol. 35, 2006, p. 517.

7 K.W. Ruyter, *The example of adoption for medically assisted conception*, in D. Evans (Ed.), *Creating the Child. The ethics, law and practice of assisted procreation*, Martinus Nijhoff, The Hague, 1996, p. 180.

ralism of family structures'[8]. Single parents, same-sex couples and older women are now able to have children and to found a family.

As Waldman states: 'for some, the explosion of ART-inspired families is cause for celebration; for others, it signals the subversion of important social values. But regardless of whether one embraces or reviles the trend, the proliferation of non-traditional baby-making poses a multitude of questions'[9].

This paper aims at analysing one of these issues, namely the right to know one's own origins. This question is relevant in any case of 'third-party reproduction', namely techniques in which genetic material or gestation is provided by a person other that the parent(s) who will take care of the resulting baby. These include:

a) heterologous fertilization, entailing sperm or egg donation and, more recently, the 'spindle transfer', a genetic manipulation technique consisting in the use of the future mother's nuclear DNA and the mitochondrial DNA coming from a donor[10];
b) embryo donation, in which leftover embryos - produced *in vitro* during a fertility treatment but not implanted in the maternal womb - or embryos specifically created for donation (using donor eggs and donor sperm) are provided to future parent(s);
c) surrogacy, involving a woman (the surrogate) carrying the pregnancy for intended parents; in this case, a third donor's oocyte is usually used to produce the embryo; more rarely the surrogate mother donates her ova. In few cases, the oocyte comes from the social mother, the woman who will take care of the resulting baby.

Whenever half of, or the entire genetic makeup comes from donors, resulting children might nourish an interest in knowing certain data of their biological ascendants, in order to assess their *genetic* origins. In addition, in case of surrogacy, resulting children might be interested in knowing other

8 M. Sabatello, *op. cit*., p. 75.
9 E. Waldman, *op. cit*., p. 517.
10 This technique aims at preventing mitochondrial diseases: P. Amato, M. Tachibana, M. Sparman, S. Mitalipov, *Three-Parent IVF: Gene Replacement for the Prevention of Inherited Mitochondrial Diseases*, in *Fertility and Sterility*, vol. 101, 2014, pp. 31-35.

relevant circumstances of their birth, even when they are not genetically related to the surrogate. As their existence would not have been possible without the surrogate's contribution, some of her data might appear essential to them, to retracetheir*biographical* origins.

4. Genetic origins in the post-genomics era: New needs generated by new technologies

Developments in medical science not only help to overcome barriers seemingly undefeatable, they also drive important changes in the society's prevalent perceptions. As a matter of fact, while ART permit to 'accord'parentingto people who would not otherwise have a genetically related offspring, the possibility to trace one's own genetic identity through a DNA test, feedsan'in-built need to know the "truth"of [each one's] origins'[11].

A critical role in this regard has been played by the Human Genome Project, a publicly funded program initiated in 1990, with the objective of determining the DNA sequence of the entire euchromatic human genome, and declared complete in 2003[12]. The consequences of this achievement are visibly enormous: the capacity to genetically predict personal risks of diseases and responsiveness to drugs, as well as the possibility to develop gene-basedmedicaments are having a revolutionary impact on the practice of medicine[13], but also on personal expectations. Since a detailed analysis of

11 J. Fortin, *Children's right to know their origin-too far, too fast?*, in *Child and Family Law Quarterly*, vol. 21, 2009, p. 341.

12 The majority of the funding for the United States human genome project came from the US Department of Energy and the National Institute of Health. The program later evolved into an international effort involving research facilities in France, Germany, Japan, the United Kingdom and the United States.

13 F.S. Collins, V.A. McKusick, *Implications of the Human Genome Project for Medical Science*, in *JAMA*, vol. 285, 2001, pp. 540-544. Since the beginning, the Human Genome Project supported an ethical, legal and social implications research program to address the many complex issues that might arise from this science. See J.E. McEwen, J.T. Boyer, K.Y. Sun, K.H. Rothenberg, N.C. Lockhart, M.S. Guyer, *The Ethical, Legal, and Social Implications Program of the National Human Genome Research Institute: Reflections on an Ongoing Experiment*, in *Annual Review of Genomics and Human Genetics*, 2014, pp. 481-505. Much attention has been paid on the possible misuse of genetic information, in particular resulting in discrimination in the field of health or

the genetic makeup explains current pathological conditionsand predicts likely future developments, knowing one's own origins implies a better treatmentand a more likely successful prevention of diseases. As a consequence, people consider this information basilar to preserve health and, more in general, to enjoy a full psycho-physical wellbeing.

Additionally, the entrance 'into the new genetic era, marked by the Human Genome Project'[14] alimented the idea that biological origins are crucial to define identity and kinship ties: the meaning of tracing one's own origins is closely linked to the construction of the self, through a complete definition of the individual's narrative identity[15]. Clearly this process is not free from potential deviations. In a society 'obsessed with tracing its ancestors'[16], 'the gene has been seen as the "unifying concept" of the field of biology, with a virtually "iconic status" that makes it capable of explaining us to ourselves'[17] and DNA has become 'a contemporary soul, the site of identity and self'[18]. As a consequence, 'people tend to see genetic information as more definitive and predictive than other types of data'[19]. Such genetic determinism or essentialism[20]generates 'an un-warranted sense of inevitability'[21] and may finally cause the risk to perceive blood kinship as superior to

insurances, as well as in the workplace: E. Wright Clayton, *Ethical, Legal, and Social Implications of Genomic Medicine*, in *New Engl J Med*, vol. 349, 2003, p. 563.

14 T. Freeman, M. Richards, *DNA Testing and Kinship; Paternity, Genealogy and the Search for the 'Truth' of our Genetic Origins*, in F. Ebtehaj, B. Lindley, M. Richards (eds.), *Kinship Matters*, Hart Publishing, Oxford, 2006, p. 79.

15 Narrative identity is 'the internalized and evolving story of the self that a person constructs to make sense and meaning out of his or her life': D.P. McAdams, *Narrative identity*, in S.J. Schwartz, K. Luyckx, V.L. Vignoles (eds.), *Handbook of identity theory and research*, Springer, New York, 2011, p. 99.

16 J. Fortin, *op. cit.*, p. 343.

17 N. Cahn, *Children's interests and information disclosure: who provided the egg and sperm? Or mommy, where (and whom) do I come from?*, in *Georgetown Journal of Gender and the Law*, vol. 2, 2000, p.17.

18 D. Nelkin, M. S. Lindee, *The DNA mystique. The Gene as a Cultural Icon*, University of Michigan Press, Ann Arbor, 2004, p. 49.

19 E. Wright Clayton, *op. cit.*, p. 563.

20 'A concept which suggests that a person is merely the sum of her genes, and behavior can be predicted based on genetic information': N. Cahn, *op. cit.*, p. 17.

21 E. Wright Clayton, *op. cit.*, p. 563.

adoptive relationships[22], or push children 'to find their "parents", not necessarily because of a"natural" desire to know their origins, but because such a desire is constructed, recognized, and legitimized by the law'[23].

Despite these questionable profiles - as a matter of fact - since the assessment of certain scientific data is becoming an easy and fast process, seeking this kind of information is rapidly turning ina routine expectation for everyone.

5. Surrogacy and biographic origins

The central importance of genetic information for health and personal identity, however, does not exhaustively explain the contents of the right to know one's one origins.

If one considers the case of adoptees trying to trace their origins, it is interesting to notice that they are usually more interested in finding the birth mother, rather than both the biological parents. As CAHAN explains, 'genetics provides only a partial explanation for the search process'[24]. As well in the case of ART-conceived people, despite the importance to be attached to DNA, the knowledge of the origins may implies an additional dimension, covering otherrelevant circumstances of birth, with special reference to the role played by surrogate mother. Depending upon personal attitude and experience, an individual might feel necessary (or at least desirable) to know the woman who has carried him or her in her womb, in order to better define the perception of the self and the scope of his/her narrative identity.

While dealing with a different issue, the ECtHR case-law seems to confirm this conclusion in *Gaskin v. UK*, stressing the existence of 'a vital interest, protected by the Convention, in receiving the information necessary to know and to understand (…) childhood and early development'[25].The case

22 N. Cahn, *op. cit*., p. 17.

23 I. Turkmendag, R. Dingwall, T. Murphy, *The Removal of Donor Anonymity in the UK: The Silencing of Claims by Would-be Parents*, in *Int'l J. of Law, Policy and the Family*, vol. 22, 2008, 291.

24 N. Cahn, *op. cit*., p. 18.

25 European Court of Human Rights, *Gaskin v. United Kingdom*, n. 10454/83, 7 July 1989, para. 49.

concerned the right of the applicant, who had been placed in public care as a baby, to have access to his complete personal file. In line with the Commission, attesting that 'the information compiled and maintained by the local authority related to the applicant's basic identity, and indeed provided the only coherent record of his early childhood and formative years'[26], the Court decided that people in the applicant's position should not be obstructed from accessing their records. *Mutatis mutandis*, a similar principle is applicable in the case of surrogacy, especially considering that prenatal attachment[27] to the gestational mother might be relevant for the definition of the individual identity.

6. The right to know one's own origins as a fundamental right to be balanced with other prominent positions

Even in the absence of an autonomous formulation in international treaties, the right to know one's own origins falls within the scope of several rights: the child's right to know his/her parents and to preserve identity, the right to a private life and to the protection of personal data and the right to health.

None of them, however, is absolute: a balance needs to be found with other (collective and individual) interests relevant in each case. Particular attention should be firstly paid to the position of donors and surrogate mothers, who may claim a right to anonymity. The right to remain unidentified is connected to the protection of their personal data, but it also aims at protecting their private and family life, whenever theywant to preserve affective ties from external interference. As much important arethe rights of social (and legal) parents, who usually wish to maintain the donors' and surrogates' anonymity, in order to better preserve the stability of their relationships with children[28]. Finally, natural siblings are in a controversial po-

26 *Ibidem*, para. 39.

27 M. Laxton-Kane, P. Slade, *The role of maternal prenatal attachment in a woman's experience of pregnancy and implications for the process of care*, in *Journal of Reproductive and Infant Psychology*, vol. 20, 2002, pp. 253-266.

28 C. Campiglio, *Norme italiane sulla procreazione assistita e parametri internazionali: il ruolo creativo della giurisprudenza*, in *Rivista di diritto internazionale privato e processuale*, vol. 50, 2014, p. 515; Id., *Procreazione assistita e famiglia nel diritto internazionale*,

sition. On the one hand, they (should) have an objective interest in knowing people sharing -at least in part - their genetic make-up, at any rateto avoid accidental incest. On the other hand, they might demand respect for their private life, including personal data.

The analysis will proceed considering the right to know one's own origins through the lens of the different international law provisions covering it. It will then move to envisage potential guidelines for a fair balance with the donors' and/or surrogates' right to anonymity, understood as a right to the respect of private life and personal data.The ECtHR case-law will offer some directions in this regard.While the Court has never decided a case on the right of ART-conceived people to know their origins, principles can be derived from the jurisprudence on the establishment of paternity and on the identification of the birthmother in case of anonymous and secret birth. In both classes of judgements, the Court affirms that people seeking to establish the identity of their ascendants have a vital interest in receiving the information necessary to establish an important aspect of their personal identity[29], and that such interest does not decrease with age, quite the reverse[30].

5.1 A multifaceted right

First of all, the right to know one's own origins can be understood as a specification of the guarantee framed under art. 7 of the Convention on the rights of the child (Child Convention), according which any child shall have, 'as far as possible, the right to know and be cared for by his or her parents'. This provision has to be broadly interpreted, in particular considering that the term 'parents' embraces genetic parents, birth parents[31]

Cedam, Padova, 2003, p. 152.

29 European Court of Human Rights, I Chamber, *Mikulić v. Croatia*, n. 53176/99, 7 February 2002, para. 64.

30 European Court of Human Rights, III Chamber, *Jäggi v. Switzerland*, n. 58757/00, 13 July 2006, para. 40; II Chamber, *Godelli v. Italy*, n. 33783/09, 25 September 2012, para. 56.

31 That is 'the mother who gave birth and the father who claimed paternity through partnership with the mother at the time of birth (or whatever the social of father is within the culture: the point being that such social definitions are important to children in

and even 'psychological parents', namely 'those who cared for the child for significant periods during infancy and childhood'[32].

However, the wording 'as far as possible' suggests that the identity of a parent may be unknown for a number of reasons[33], including cases in which the State itself decides that a parent should not be identifiable (so-called 'state-approved secrecy')[34]. Thus, art. 7 'create[s] a presumption in favour of providing children with access to information about their biological parents before they turn 18 where this is logistically possible, that is, if the information is available'[35]. Worthy of note, egg/sperm donation under anonymity (whenever prescribed or consented by domestic law) is a state-approved secrecy: nevertheless, the UN Committee on the rights of the child argued the possible contradiction between this policy and art. 7[36].

The right to know one's own origins is also linked to the right to preserve identity, guaranteed by art. 8 of the Child Convention. This provision contains the first legal recognition of identity as a fundamental right and, notably, at the benefit of children[37]. This notwithstanding, article 8 does not provide a sound definition of identity, but it rather mentions three of the aspects that this concept includes (name, nationality and family relations), already enumerated under art. 7. Still, this is not an exhaustive list as 'many other aspects of the child's identity (…) are deemed protected by the provi-

terms of their identity)': UNICEF, *Implementation Handbook for the Convention on the Rights of the Child*, 2007 pp. 104-105.

32 *Ivi*, p. 105.

33 For example, when the mother does not know who the father is, the child has been abandoned or, the mother refuses to identify the father: 'while mothers could, arguably, be legally required to name the father, it would be difficult to enforce this and conflict could be raised between the mother's rights and the child's rights'. *Ivi*, p. 135.

34 *Ibidem*.

35 J. Tobin, *Donor conceived individuals and access to information about their genetic origins: the relevance and role of rights*, Melbourne Legal Studies Research Paper n. 591, 2002, p. 13, available at: http://papers.ssrn.com.

36 UN Committee on the rights of the child: CRC/C/15/Add.23 (Norway) 25 April 1994, para. 10; CRC/C/15/Add.182 (Switzerland) 13 June 2002, paras. 28 e 29; CRC/C/15/Add.188 (United Kingdom) 9 October 2002, paras. 31 e 32.

37 G.A. Stewart, *Interpreting the Child's Right to Identity in the U.N. Convention on the Rights of the Child, in Family Law Quarterly, vol. 26, 1992, pp. 221 ss.*

sion, for example the child's personal history, (…) race, culture, religion, language and (…) physical appearance, abilities and inclinations'[38]. As a matter of fact, 'identity' is a very broad concept covering all those elements that allow anyone to assert his/her existence in a society. Identity is a matter of recognition of everybody's individuality, what differentiates any person from his/her peers. Thus, article 8 includes 'the right to know one's ancestral background, including medical and genetic information about oneself and one's biological parentage, the circumstances of one's conception, time and place of birth, and records of other events meaningful to the individual'[39].

Children, obviously, are not the only beneficiaries of the right to know the genetic and/or biographic origins. Rather, this right is more easily exercised in adulthood: therefore, other treaty provisions are relevant to assess it.

The right to trace one's own origins is connected to the right to the respect of private life, guaranteed by art. 8 of the European Convention of Human Rights (ECHR), as well as by art. 7 of the Charter of Fundamental Rights of the European Union (EU Charter), and by many other provisions, even under the different wording of 'right to privacy'[40]. As clarified by the European Court of Human Rights, the right to the private life covers many different manifestations of a person's existence, seen both as an expression of individuality and as a set of relationships with other people. It is clear that access to information on genetic and biographic origins may significantly influence the harmonious development of each individual's personality, conditioning the way of being of each one, as well as the establishment of connections with others.

The right to know one's own origins can also be construed as part of the right to the protection of personal data, guaranteed under art. 8 ECHR and specified in other provisions, such as art. 8 of the EU Charter. This right implies a positive obligation upon States to ensure in favor of any individual

38 S. Besson, *Enforcing the Child's Right to Know Her Origins: Contrasting Approaches Under the Convention on the Rights of the Child and the European Convention on Human Rights*, in *International Journal of Law, Policy and the Family*, vol. 21, 2007, pp. 143-144.

39 *M. Freeman, A. Margaria,* Who and What Is a Mother? Maternity, Responsibility and Liberty, in Theoretical Inquiries in Law, vol. 13, 2012, pp. *159-160.*

40 Universal Declaration of Human Rights, 1948, art. 12; International Covenant of Civil and Political Rights, 1966, art. 17.

the access to his/her data, held by public authorities or private persons.

Last but not least, the right to know one's own origins is closely related to the right to health, which is founded on a number of different legal provisions, both in universal[41] and in regional instruments[42]. While being a dynamic concept, involving technical and legal different interpretations[43], the right to health certainly includes the right to have access to relevant information including family medical history, which is particularly important in the case of hereditary diseases. This precise profile is explicitly recognized under art. 10 of the Oviedo Convention, stating that 'everyone is entitled to know any information collected about his or her health'.

5.2 Possible guidelines for balancing competing interests

To identify guidelines for a fair balance between the rights to know genetic/biographic origins and other competing interests, it should be firstly considered whether the person interested in tracing his or her origins is a child or not.

As a matter of fact, whenever a minor (once became mature enough) claims to exercise the right to know his/her genetic/biographic origins, the principle of 'the best interest of the child'should be applied to solve potential clashes with competing interests.This principle, envisaged by art. 3 of the Child Convention, implies that the child's best interest shall be a primary consideration in all actions concerning children taken both by state authorities and by private institutions. The UN Committee on the rights of the child has clarified that it is a threefold concept, being at the same time a substantive right, an interpretative legal principle, and a rule of proce-

41 Universal Declaration of Human Rights, 1948, art. 25; International Covenant of Economic, Social and Cultural Rights and Political Rights, 1966, art.12; International Convention on the elimination of all forms of racial discrimination, 1965, art. 5; Convention on the elimination of all forms of discrimination against women 1979, art. 11 and art. 14; Convention on the rights of the child, 1989, art. 24.

42 American Declaration of the rights and duties of man, 1948, art. XI; Additional Protocol to the American Convention on human rights in the area of economic, social and cultural rights, 1988, art. 10; African Charter on human and peoples' rights, 1981, art. 16; European Social Charter, 1996, art. 11.

43 P. Acconci, *Tutela della salute e diritto internazionale*, Cedam, Padova, 2011, p. 5.

dure[44], while the ECtHR confirms that it is the guiding principle that drives its decision whenever a child's position is considered[45].

Despite its undisputed relevance, 'the definition of the child's best interests, (…) is not always obvious, especially in a long-term perspective. (…) [I]t has been argued that what is in the best interests of the child varies from one era to another and also depends on the resources, the developmental level and the culture of the country in which the child lives'[46]. In this sense, one might conclude that the child's interest should be specifically qualified in light of the features of the case to justify the disclosure of relevant data, for example when special health reasons militate for a full tracing of the genetic origins.

Nevertheless, in the most recent ECtHR's case-law, this principle seems to push the Court to identify not only a right, but even a 'duty' to know one's origin.This is what emerges from the case *Mandet v. France*[47], in which the domestic courts acknowledged the right of a presumed biological father to have his paternity recognized, deciding that this was in the son's best interests, despite the child (who already had a legal and social father) asked the judges not to change his established family ties. The child claimed a violation of art. 8 before the Court,which ratherconfirmed the domestic authorities' decision, arguing - as underlined by MERCKX -that 'the interests of the son simply did not lie where he saw them'[48]. According to the Strasbourg judges, domestic courts did not make the position of the biological fatherprevail over the child's ones, but rather they correctly considered that

44 UN Committee on the rights of the child, General Comment No. 14 on the 'Best Interests of the Child', CRC/C/GC/14, 29 May 2013.

45 European Court of Human Rights, V Chamber, *Mennesson v. France*, n. 65192/11, 26 July 2014, paras. 99-100; *Labasseev. France*, n. 65941/11, 26 July 2014, paras. 78-79.

46 T. Hammarberg, *The principle of the best interests of the child – what it means and what it demands from adults*, CommDH/Speech(2008)10, 30 may 2008, at: https://wcd.coe.int/ViewDoc.jsp?p=&id=1304019&direct=true.

47 European Court of Human Rights, V Chamber, *Mandet v. France*, n. 30955/12, 14 January 2016.

48 E. Merckx, *Mandet v. France: Child's "duty" to know its origins prevails over its wish to remain in the dark*, available at https://strasbourgobservers.com/2016/02/04/mandet-v-france-childs-duty-to-know-its-origins-prevails-over-its-wish-to-remain-in-the-dark/#comments.

the interests of both converged[49].

Differently, when the rights of an ART-conceived adult are at stake, it would firstly be necessary to draw a distinction between non-identifying and identifying data, as the precise contents of the information appears diriment.

In fact, the disclosure of non-identifying data would easily satisfy the interest of the ART-conceived person, while preserving the right to anonymity of the other people involved. This is particularly relevant if one consider the right to health of the ART-conceived person. Despite de-anonymization of gamete donors[50] is usually the best way to guarantee access to genetic information - a key tool in the prevention and treatment of diseases - alternative solutions are certainly feasible[51]. In fact, 'sperm banks have endeavored, and government regulation thereof should push, to make available to the parents of donor-conceived children the fullest possible medical histories'[52]. Thus, the right to health of ART conceived person can be satisfied without any interference in the rights of donors/surrogate, in particular without revealing their identity. The disclosure, in this case, should probably include the constant updated of the relevant records, possibly 'contractually enforceable by banks against sperm donors'[53], which appears an opportune and necessary operation in view of the constant scientific development in detecting diseases and producing medicaments.

On the contrary, much more controversial would be the disclosure of the donor's and/or the surrogate mother's identity.

A possible normative solution could be drawn from the ECtHR's case-law on anonymous and secret birth. The decisions held in the cases *Odièvre*

49 European Court of Human Rights, *Mandet v. France cit.*, para. 57.

50 In this case the role of surrogate is probably less relevant, unless for health problems arisen during the gestation.

51 A. Cameron, V. Gruben, F. Kelly, *De-anonymising sperm donors in Canada: some doubts and* directions, in *Canadian Journal of Family Law/Revue canadienne de droit familial*, vol. 26, 2010, p. 110.

52 I. Glenn Cohen, *Sperm and Egg Donor Anonymity: Legal and Ethical Issues*, in L. Francis,*Oxford Handbook of Reproductive Ethics*, Oxford University Press, 2016, available at: http://ssrn.com/abstract=2600262, p. 15.

53 *Ibidem*.

v. France[54] and *Godelli v. Italy*[55], demonstrate that the Court, in order to balance the right to anonymity of the birthmother and the right to trace origins of the progenies, requires an independent and impartial mechanism aimed at verifying, at the request of the interested person, the mother's availability to waive anonymity[56]. Therefore, it is up to the birthmother to decide whether (and to what extent) to renounce to confidentiality: in fact, anonymous and secret birth is usually permitted to preserve not only the mother's and child's health during pregnancy and birth, but also to avoid abortions, abandonment other than under the proper procedure and even infanticide[57].

However, anonymity has clearly not the same meaning under ART normative discipline. Moreover, as Bottis well explains, 'withholding a secret from someone represents the power over that person and a conflict of interest between two parties'[58], especially when the information is kept reserved '"from the very person" [it] is directly related'[59]. If one considers that 'the donor-conceived person [could] insist that the biological father's/donor's personal data are simultaneously 'her' data as well'[60], the request to get information would not be described as the access to another individual's personal data and would be consequently more easily satisfied.

Nevertheless, 'the rules on anonymity versus mandated identification are likely to be at the center of [the donor's] evaluation in the majority of cases'[61]. For this reason, while a 'prospective' regime, requiring for future donations/surrogacies the disclosure of all identifying information, would certainly not interfere with a surrogate/donor's right to anonymity[62], the

54 ECtHR 2003 – 111 (2003), ECtHR (2004). 38 EHRR43.

55 (2012) ECHR 33783/09.

56 European Court of Human Rights, *Godelli v. Italy cit*., para. 57; Grand Chamber, *Odièvre v. France*, n. 42326/98, 13 February 2003, para. 49.

57 European Court of Human Rights, *Odièvre v. France cit*., para. 45.

58 M. Bottis, *Anonymization of Sperm Donors for artificial insemination: an international data protection law perspective*, in *Icfai University Journal of Environmental & Healthcare Law*, vol. 8, 2009, p. 75.

59 *Ibidem*.

60 *Ivi*, p. 80.

61 I. Glenn Cohen, *op. cit*., p. 16.

62 In fact, those who do not wish to be identified may simply choose not to donate their gametes or be a surrogate.

legitimacy of the opening of past records ('retrospective' regime) is much more debated. A possible solution would be permitting retrospective access to identifying information, allowing the donors/surrogates to veto any potential contacts with the resulting children (so-called 'contact veto system'[63]). However, according to Tobin, 'the compulsory release of identifying information against the will of a donor, even where a contact veto is in place and the donor conceived individual faced the threat of criminal sanction should this veto be breached, still remains problematic, [as it would] violate the guarantee of anonymity given to the donor in circumstances where it was a condition precedent to him making the donation in the first instance'[64].

Therefore, the States are certainly called under international law to regulate the access to identifying information for future donations/surrogacies, but they should maintain the option of confidentiality for donors and surrogateswho have been guaranteed anonymity, while encouraging them to disclose their identity.

5.3 The duty to tell the truth as a parents' responsibility: what role for the State?

The right to know one's own origins certainly implies the right to be informed about the modalities of the conception, namely through the use of one of the mentioned techniques. We can define this profile as 'the right to the truth': it represents an essential prerequisite to the exercise of the right to know one's own origins. In this field, children of heterosexual recipient parents are more exposed to a denial of their right than children of same-sex and single parents. As a matter of fact, secrecy surrounding the use of third-party ART is quite common among heterosexual couples and it is driven by a number of fears concerning possible negative impact on family bonds, especially between the parent who lack a genetic link with the child and the child himself/herself[65]. On the contrary, a number of factors

63 S. Allan, *Access to information about donors by donor-conceived individuals: A human rights analysis*, in *Journal of Law and Medicine*, vol. 20, 2013, p. 669.

64 J. Tobin, *op. cit.*, p. 26.

65 A. Cameron, V. Gruben, F. Kelly, *op. cit.*, pp. 130-131.

explains the reason why lesbian and gay parents not only reveal the gamete donation (as well as surrogacy, when used), but the identity of the donor or surrogate mother as well[66].

Does 'the right to the truth' imply a duty upon the States to 'enforce' the information?

If the answer were in the positive, a mechanism making information available to the resulting child only at his/her request, would not be sufficient for the State to fulfill its obligation. Rather, an 'active registry' would be necessary: 'a more muscular kind of intervention, which (…)would itself contact the child at age eighteen to let him or her know that he or she was donor conceived and allow (but not force) him or her to receive information about the donor'[67].

A similar solution does not appear desirable, as it creates more problems than those it aims to address. Therefore, 'the right to the truth', as a *conditio sine qua non* for the exercise of the right to know the genetic and biographic origins, rests upon the parents who will freely decide whether to be honest with their children about the nature of their conception or not. In this field, the States play only a residual role, being called to encourage parents to reveal to their children that they are donor-conceived, and to possibly supplycounselling services that may assist and guide all the people involved in the disclosure process, if needed.

7. Conclusions

The respect of the right to know one's own origins requires rules imposing to donors and surrogates the disclosure (and, to some extent, the constant updating) of non-identifying data, including medical records, and even of identifying information, at least for donation and surrogacy to come. Donors' and/or surrogates' anonymity deserves a more stringent protection, when they have been guaranteed confidentiality, but States are arguably called to envisage mechanisms to encourage the release of information, as well as sustaining social parents and children in the process of disclosure

66 N. Cahn, *op. cit.*, pp. 14 ss.

67 I. Glenn Cohen, *Rethinking sperm-donor anonymity: of changed selves, nonidentity, and one-night stands*, in *Georgetown Law Journal*, vol. 100, 2012, p. 447.

the means of conception.

The recourse to ART is usually justified by the parents' desire to have (at least partial) genetic connection with their progenies, as 'a biological connection to the future' is considered 'a vital part of the identity of adults'[68]. Similarly, and even *a fortiori*, children might feel the analogous desire to define their 'biological connectedness to the past'[69], as well as other elements of their personal history, including pre-natal experiences, as in the case of surrogacy. The States are thus called to guarantee that the use of technologies to create children and families is accompanied by clear normative provisions, fairly guaranteeing rights and interests of everybody.

68 N. Cahn, *op. cit.*, p. 19, quoting J. Lindemann Nelson, *Cloning, Families, and the Reproduction of Persons*, in *Valparaiso University Law Review*, vol. 32, 1998, p. 719.

69 *Ibidem*.

ETHICS

Awareness and Knowledge of Cyberethics by Library and Information Science Doctoral Students in Two Nigerian Universities

by Airen Adetimirin[1]

1. Introduction

Doctoral students study to acquire a doctoral degree from a university and are assigned supervisors who oversee their research. The duration of this programme is about three or more years, at the end of which they examined by a panel of examiners which includes: the external examiner who does not belong to that university, but is a recognized academic in the area of the candidate's research, an internal examiner who is a member of staff in the same university, the supervisor(s), the head of the department, the representative of the postgraduate school and others. The panel members determine if they are qualified to be awarded the doctoral degree.

Library and Information Science (LIS) doctoral students are students who are studying for a doctoral degree in Library and Information Science discipline on full or part time basis and may teach in a library school, work in a library, information centre or any other organization or as a consultant at the end of their programme. LIS doctoral students will, therefore, need information for their research, writing seminar papers and other academic activities (Abubakar and Adetimirin, 2015). Ismail et al. (2011) emphasized the importance of research to postgraduate students and this necessitates searching for information from different sources as books, journals, databases, the internet, library and others. The need to retrieve current and relevant information whenever it is required has prompted the use of elec-

1 Lecturer, Department of Library, Archival and Information Studies, University of Ibadan, Ibadan, Nigeria, Email: aeadetimirin@gmail.com; ae.adetimirin@ui.edu.ng.

tronic resources which are easily accessible from anywhere (Swamy and Kishore, 2013; Sinha, et al., 2011).

LIS doctoral students also need to access their university portal to register, pay school fees, learning management systems, read bulletin, get latest news or information about their university, conferences, seminars, workshops, and programmes. Access to the university portal and electronic resources is made possible by Information and Communication Technology (ICT) which include the Internet, computers, Laptops, IPods, Tablets and smart phones. Doctoral students may now easily access these electronic resources through these ICT from different access points such as library, computer laboratory, classroom, department, home and offices. The ethics about using ICT by these students for their programme becomes imperative and this is what is referred to as cyberethics.

Cyberethics is a broader term than computer ethics and internet ethics (Onyancha, 2015).

Rama (2014) defined cyberethics as the "rules set out for responsible behavior in cyberspace and it explores the guideline for online conduct that influences the social, political, legal and business affairs". Igwe and Ibegwam (2014) explained cyberethics as the "social responsibility in cyberspace", while is seen as a "discipline of using appropriate and ethical behaviors and acknowledging moral duties and obligations pertaining to online environments and digital media" (IKeepSafe, 2014). Ramadhan, et. al. (2011) described as a system of standards that prescribe morality and immorality in cyberspace, signifying the preservation of freedom of expression, intellectual property and privacy.

Igwe and Ibegwam (2014) highlighted some cyberethical issues to include: "plagiarism, copyright, hacking, fair use; file sharing, online etiquette protocols, posting incorrect/inaccurate information, cyber-bullying, stealing or pirating software, music, and videos, online gambling, gaming, and internet addiction. Others are privacy, security, electronic monitoring of employees, collection and use of personal information on consumers, and identity theft".

LIS doctoral students need to be aware of cyberethics as they source for different information especially from the Internet such as open access journals, online databases, videos, photographs. Therefore, they must know about the ethical use of these information resources to avoid violat-

ing them in terms of referencing by acknowledging the author and source from where they got the information sources, plagiarism and copyright infringement. It is only when students are aware and possess the cyberethics knowledge guiding these information resources, that they can use these information resources legally and morally.

Literature revealed that unethical use of ICT by students (primary, secondary undergraduates and postgraduate) and lecturers is a major challenge in educational institutions (Özer et al., 2011; Ki and Ahn, 2006; Johnson and Simpson, 2005). Beycioglu (2009) and Akbulut et al. (2008) reported that the Turkish educational institutions are faced with the challenge of unethical use of computers and suggested that teachers should educate students on the ethics of using ICT. Johnson and Simpson (2005) reiterated the importance of understanding the legal and illegal use of computer by lecturers or researchers and this was also affirmed by Özer et al., (2011) who investigated computer teachers' attitude towards ethical use of computers in elementary schools in Turkey.

Igwe and Ibegwam (2014) affirmed that cyberethics education is necessary and should be taken with much importance in Nigeria as it will facilitate the integration of moral and responsible behavior of the citizens (children, youth and adults) in the use of the Internet and surfing the cyberspace. They defined cyberethics education as an "instructional programme that is aimed at inculcating in individuals knowledge of ethical standards and issues required while using the cyber space in order to avoid acts that constitute cybercrimes, which are punishable by law". Therefore, LIS doctoral students must be knowledgeable on cyberethics in their use of electronic information resources for their programme to avoid contravening any law or regulation relating to the use of electronic information resources retrieved from the Internet.

2. Statement of the problem

LIS doctoral students use ICT to retrieve information required for their research and various academic activities. The use of ICT is guided by rules and their awareness and knowledge of these rules will justify their adherence to such rules. After graduation, these doctoral students graduation will become custodians of information expected to acquire, organize, dis-

seminate information to users and should abide by the ethics guiding the use of ICT. Their adherence to ethics will be determined by their awareness and knowledge of the ethics guiding the use of ICT which is referred to as cyberethics. The level of awareness of LIS doctoral students in Nigerian universities about cyberethics has not been adequately researched. Therefore, this study investigated the current level of awareness and knowledge that LIS doctoral students have about cyberethics.

2.1 Research questions

The following questions guided the research:

1. What is the level of awareness of cyberethics by LIS doctoral students?
2. How knowledgeable are doctoral students about cyberethics?
3. What is the adherence of the doctoral students to cyberethics using PAPA framework (property, accuracy, privacy and access)?

2.2 Theoretical framework

PAPA framework is the anchor for this study. PAPA framework was conceived by Mason (1986) about the personal harm that may result from the unethical use of information technology and it has four categories that deal with ethical issues for the information age: privacy, accuracy, property and access (PAPA). Woodward et al., (2010) reported that these four categories are still relevant and explained privacy as the ability of an individual to decide what information to keep secret, what to share and that what is shared will be confidential. Accuracy dealt with who was responsible for information being accurate and authentic and retribution should be done to those who were negatively affected through erroneous data or information. Property in the framework involves "intellectual property rights, including those not necessarily protected by law" and physical property such as the information carriers. This identifies who owes information and how compensation is determined. Access "dealt with the right or authority to obtain information" (Woodward et al., 2010).

Different studies have investigated one or two of PAPA constructs, but Conger et al. (1995) as reported by Woodward et. al. (2010) considered all

four constructs. Conger et al. (1995) analysed twelve factors which they classified into five groups and reported that three of Mason's construct, privacy, access and property, aligned with their findings, although property was defined as concept of ownership. The fourth group was different from Mason's as it considered "responsibility for accuracy", while the fifth one was motivation which Mason did not include in his construct.

Harris (2000) developed his instruments around Mason's PAPA and measured student attitudes towards IT related ethical issues and found that there was an increase in sensitivity towards IT ethical issues as academic training increased. Another study by Peslak (2006) on 200 individuals affirmed that the four original PAPA issues were still timely and relevant ethical concerns. The four issues in PAPA framework are relevant to LIS doctoral students who will graduate and become information professionals, managers of information centres or lecturers who have to ensure that cyberethics is endorsed by themselves and their users or clients.

2.3 Methodology

The descriptive survey was used and the population consisted of 81 Library and Information Science (LIS) doctoral students from two universities in Nigeria: University of Ibadan and University of Ilorin. The LIS doctoral students from University of Ibadan were 70, while those from University of Ilorin were 11. The eighty one doctoral students in both universities constituted the sample size, Questionnaire was adapted from the cyberethics scale by Supavai (2014) which explained the PAPA framework. Analysis was done using frequency, percentages and cross tabulation.

4. Results and discussion

Table 1 is on the demographic information of the respondents. It revealed that there are more female respondents in the study in both universities (37 females and 28 males) and none of the respondents were less than 30 years old. However in Ibadan, the oldest respondent was more than 54 years, while the oldest respondent in Ilorin was in the age range of 45-49 years. In both universities, no respondent registered for MPhil programme, but the respondents in Ibadan registered for both Mphil/PhD (29.6%) and PhD (70.4%), while all the respondents in Ilorin were registered for PhD pro-

gramme (100%).

Table 1. Demographic Information of Respondents

Variables		Ibadan		Ilorin	
		N	%	N	%
Gender	Male	24	44.4	4	36.4
	Female	30	55.6	7	63.6
Age (years)	<25	-	-	-	-
	25 – 29	-	-	-	-
	30 – 34	6	11.1	2	18.2
	35 – 39	12	22.2	6	54.5
	40 – 44	8	14.8	2	18.2
	45 – 49	14	25.9	1	9.1
	50 – 54	10	18.5	-	-
>54		4	7.4	-	-
Programme enrolled for:	MPhil.	-	-	-	-
	MPhil/PhD	16	29.6	-	-
	PhD	38	70.4	11	100.0
Years on the programme:	<1	6	10.3	-	-
	1	10	17.2	3	27.3
	2	4	6.9	3	27.3
	3	14	24.1	5	45.4
	4	6	10.3	-	-
	5	4	6.9	-	-
	6	6	10.3	-	-
	7	4	6.9	-	-
	8	4	6.9	-	-

3.1 Level of awareness of cyberethics by the LIS doctoral students

The level of awareness of cyberethics was determined through the frequencies from the statements asked in the questionnaire and documented in Table 2. The measuring scale for the level of awareness was: Very Highly Aware (VHA), Highly Aware (HA), Aware (A) and Not Aware (NA). The results indicated that all the respondents in Ilorin were aware of cyberethics, but not all respondents were aware of cyberethics in Ibadan (Table 2). When VHA and HA were merged, respondents in Ibadan were mostly

aware about intellectual property (92.6%) and respected others in an online environment (83.4%), while those in Ilorin were mostly aware of ethical issues of using ICT and social implications of ICT use (100 %). About six respondents (11.1%) in Ibadan were not aware of acceptable ICT use policy, while all the respondents in Ilorin indicated awareness in all the statements on cyberethics in Table 2.

The doctoral students in both universities were aware of cyberethics, but their level of awareness on different aspect of cyberethics varied. However, the respondents in Ilorin were more aware of cyberethics than those in Ibadan. This could be so because the programme in Ilorin is still new, about three years since it was started and the respondents are conversant with recent development in the ethics of carrying out research. The respondents in Ilorin's high level of awareness of cyberethics may also be explained that cyberethics is becoming an issue of discussion and researched upon in the last three to four years in literature. This is because of the unethical use of computer and ICT in educational institutions (Ki and Ahn, 2006).

This result is in conflict with the findings of Beycioglu (2009) who reported that students in educational institutions in Turkey are involved in unethical use of computers which meant that students are not aware of cyberethics which is the regulation guiding the appropriate use of ICT. Özer et al. (2011) concluded from his study on computer teachers' attitudes towards ethical use of computers in elementary schools in Turkey that the teachers violated the ethics of using the computers because they were not aware of such ethics guiding its use. He strongly recommended that the teachers should be taught about cyberethics throughout their programme, that is the ethics guiding the use of the Internet and other ICT and this will invariably make them abide by such ethics.

3.2 Level of cyberethics knowledge by the LIS doctoral students

On the level of knowledge of cyberethics as indicated in Table 3, less than half of the respondents were very highly knowledgeable about intellectual property in Ibadan (44.0%), while 63.6 % of those in Ilorin were very highly knowledgeable of acceptable ICT use policy. When the scale of Very Highly Knowledgeable (VHK) and Highly Knowledgeable (HK) were merged, the same trend occurred in Ibadan as 73.6% of the respondents were still

knowledgeable about intellectual property. However, the trend in Ilorin is that of high level of knowledge about intellectual property (90.9%) and responsible use of ICT as a priority (90.9%). Respondents in Ibadan were not knowledgeable of acceptable ICT use policy (11.1%), responsible use of ICT as a priority (11.1%) and social implications of ICT use (11.5%). For the scale on not knowledgeable (NK), no respondent in Ilorin was found in this group, but few respondents (2-6) in Ibadan were found in this group (Table 3).

Respondents in Ilorin were more knowledgeable in cyberethics than those in Ibadan. However, the respondents' level of knowledge about different aspect of cyberethics varied in both universities. This can be attributed to the fact that more than three quarters of the respondents in both universities were highly aware of cyberethics and this translated to their acquisition of the knowledge in their use of ICT for their research and other academic activities. This affirms the findings of Igwe and Ibegwam (2014) that cyberethics education is necessary for all citizens including doctoral students as this will facilitate good and moral behavior in their use of computer and ICT. Doctoral students with good cyberethics education will be knowledgeable in the appropriate use of ICT and may not likely violate the ethics when usingICT for their academic activities.

The result disagrees with those of Akbulut et. al. (2008) who affirmed that inappropriate use of technology in education is presently a research focus for many researchers in ethics. This is a research focus due to the observance that technology for teaching and learning is now a common phenomenon in higher institution and students and lecturers are not using technology appropriately. This could be because they do not have the requisite knowledge of cyberethics.

5. Adherence of the doctoral students to cyberethics using PAPA framework

The LIS doctoral students were examined on cyberethics using the PAPA framework by asking questions on all four issues in PAPA framework: property, accuracy, privacy and access (Table 4). The measuring scale used was a four point Likert scale measuring the importance of cyberethics on a scale of 4-1 of Strongly Agree (SA) = 4, Agree (A)= 3, Disagree (D) = 2 and Strongly Disagree (SA) = 1 and frequencies were calculated (Table 4).

Table 2 Level of Awareness of Cyberethics by the Doctoral Students

Statements	IBADAN								ILORIN							
I am aware:	VHA		HA		A		NA		VHA		HA		A		NA	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
of ethical issues of using information and communication technology	20	37.0	22	40.7	10	18.5	2	3.7	-	-	11	100.0	-	-	-	-
about intellectual property	30	55.6	20	37.0	4	7.4	-	-	5	45.4	5	45.4	1	9.1	-	-
of acceptable ICT use policy	12	22.6	26	48.1	10	18.5	6	11.1	-	-	10	90.9	1	9.1	-	-
responsible use of ICT as a priority	18	33.3	22	40.7	10	18.5	4	7.4	-	-	8	72.7	3	27.3	-	-
social implications of ICT use	18	33.3	20	37.0	14	25.9	2	3.7	-	-	11	100.0	-	-	-	-
of respecting others in an online environment	20	37.0	26	48.1	6	11.1	2	3.7	3	27.3	7	63.6	1	9.1	-	-
of privacy in the use of ICT	18	33.3	22	40.7	10	18.5	4	7.4	2	18.2	8	72.7	1	9.1	-	-
copying software or copyright violation is wrong	26	50.0	18	34.6	6	11.5	2	3.8	-	-	9	81.8	2	18.2	-	-

Table 3 Level of Knowledge of Cyberethics by the Doctoral Students

Statements	IBADAN								ILORIN							
I am knowledgeable about:	VHK		HK		K		NK		VHK		HK		K		NK	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
ethical issues of using information and communication technology(ICT)	8	15.4	24	46.2	18	34.6	2	3.8	-	-	6	54.5	5	45.4	-	-
intellectual property	24	44.4	16	29.6	14	25.9	-	-	-	-	10	90.9	1	9.1	-	-
acceptable ICT use policy	12	22.2	24	44.4	12	22.2	6	11.1	7	63.6	-	-	4	36.4	-	-
responsible use of ICT as a priority	12	22.2	26	48.1	10	18.5	6	11.1	-	-	10	90.9	1	9.1	-	-
social implications of ICT use	8	15.4	22	42.3	16	30.8	6	11.5	-	-	8	72.7	3	27.3	-	-
respecting others in an online environment	18	33.3	26	48.1	10	18.5	-	-	3	27.3	5	45.4	3	27.3	-	-
privacy in the use of ICT	10	19.2	24	46.2	16	30.8	2	3.8	-	-	9	81.8	2	18.2	-	-
copying software or copyright violation is wrong	16	30.8	26	50.0	8	15.4	2	3.8	2	18.2	5	45.4	4	36.4	-	-

On property, respondents who indicated that they often downloaded files such as videos, movies, games and songs for free from the Internet (P 1) and often share files with others (P 2) were highest when strongly agreed and agreed were merged in both Ibadan (76%, 70.8%) and Ilorin (100%). More than half of the respondents in both Ibadan (53.8%) and Ilorin (72.7%) strongly disagreed to using people's articles without acknowledging source (P 7). The result implies that doctoral students are aware of the intellectual rights of the authors and that it should be protected.

This finding indicates that the students are informed about cyberethics and its consequences for its violation and therefore, will not want to be associated with such behaviour which could negatively affect their academic pursuit if caught and brought to face the law. The high adherence to the property construct in the PAPA framework could be as a result of the high knowledge level of cyberethics possessed by the doctoral students. This result supports those of Woodward et al. (2010) who reported that property misuse occurred among Information Technology (IT) undergraduates in four countries (America, Britain, Germany and Italy) and majority of these students could be classified into the low risk property group because they misused the property construct due to the personal gain that can be accrued from using ICT and the low penalty for its consequences.

Almost all the respondents in Ibadan (92.0%) indicated that some of the information on the Internet is not renewed regularly, while all the respondents in Ilorin (100%) also agreed to this on the issue of accuracy (A5). The doctoral students need current information for their research and other academic activities and a ready source of that is the internet and when they search for information and retrieve it only to discover that such information is not current can be disturbing. Academic information should be updated regularly for these students to use. Over 75% of the respondents in both universities attested to the ability to find the required information very easily on the Internet (A 3, Ibadan: 76.9%, Ilorin: 100%). This is expected as this group of students has first and second degrees and would have acquired some information literacy skills which facilitate their ability to retrieve relevant information easily from the Internet.

Table 4: Respondents' Adherence to PAPA Framework in Cyberethics

Variable	IBADAN								ILORIN							
	SA		A		D		SD		SA		A		D		SD	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Property: P1	16	32.0	22	44.0	8	16.0	4	8.0	11	100.0	-	-	-	-	-	-
P2	10	20.8	24	50.0	14	29.2	-	-	8	72.7	3	27.3	-	-	-	-
P3	10	20.0	12	24.0	26	52.0	2	4.0	-	-	-	-	-	-	11	100.0
P4	2	3.8	20	38.5	22	42.3	8	15.4	-	-	11	100.0	-	-	-	-
P5	4	7.7	10	19.2	30	57.7	8	15.4	-	-	-	-	-	-	11	100.0
P6	2	3.8	24	46.2	22	42.3	4	7.7	-	-	-	-	11	100.0	-	-
P7	-	-	4	7.7	20	38.5	28	53.8	-	-	3	27.3	-	-	8	72.7
P8	4	7.7	20	38.5	14	26.9	14	26.9	-	-	-	-	11	100.0	-	-
Accuracy: A1	-	-	26	50.0	18	34.6	8	15.4	3	27.3	-	-	8	72.7	-	-
A2	4	7.4	14	25.9	28	51.9	8	14.8	-	-	-	-	11	100.0	-	-
A3	14	26.9	26	50.0	10	19.2	2	3.8	-	-	11	100.0	-	-	-	-
A4	-	-	4	7.7	30	57.7	18	34.6	-	-	-	-	11	100.0	-	-
A5	12	24.0	34	68.0	-	-	4	8.0	-	-	11	100.0	-	-	-	-
Privacy: PR 1	6	11.5	16	30.8	18	34.6	12	23.1	-	-	11	100.0	-	-	-	-
PR 2	12	23.1	8	15.4	20	38.5	12	23.1	-	-	-	-	11	100.0	-	-
PR 3	8	15.4	12	23.1	22	42.3	10	19.2	-	-	-	-	11	100.0	-	-
PR 4	12	23.1	8	15.4	20	38.5	12	23.1	-	-	-	-	11	100.0	-	-
PR 5	6	11.5	8	15.4	24	46.2	14	26.9	-	-	-	-	11	100.0	-	-
PR 6	12	23.1	4	7.7	16	30.8	20	38.5	-	-	-	-	11	100.0	-	-
Access: AC 1	8	14.8	20	37.0	12	22.2	14	25.9	-	-	-	-	11	100.0	-	-
AC 2	14	25.9	26	48.1	4	7.4	10	18.5	-	-	11	100.0	-	-	-	-
AC 3	10	18.5	14	25.9	16	29.6	14	25.9	-	-	-	-	11	100.0	-	-
AC 4	6	11.5	14	26.9	20	38.5	12	23.1	-	-	-	-	11	100.0	-	-

On privacy, over 70% of the respondents in both universities; Ibadan (73.1%) and Ilorin (100%) disagreed to the practice of entering other people's social networking site without authorization (PR 5) and the highest number of respondents in Ibadan (69.3%) and all in Ilorin were found not to use other people's password to access information from the Internet (PR 6). The doctoral students are aware of the relevance of privacy of people's rights and not violate against such rights by using sites or password without permission. The findings reveal that the LIS doctoral students are knowledgeable about protecting the privacy of other individuals. With the increased use of the Internet which enables access to so much information, it is important that the doctoral students realise the importance of protecting the rights of individuals in their use of the Internet and other ICT. This aligns with Mason's (1986) privacy issue, Conger et al. (1995) and Woodward et. al. (2010) who all strongly recommended that the right of an individual should be protected when using ICT.

When access was considered, only 74% of the respondents in Ibadan and all in Ilorin indicated that they do not use unauthorized banned website (AC 2), while only about half of those in Ibadan (51.8%) and none in Ilorin accessed the Internet freely in their institution (AC 1). This reflects that the respondents knew the implication of using a banned website and that accessibility to information on the internet was hindered when the doctoral students were in their universities as it involves paying a fee to access the internet.

The study by Peslak (2006) on Mason's framework using faculty, students and administrators as respondents revealed that the four issues: property, accuracy, privacy and access were still relevant after two decades that Mason's framework was discovered. The author also found out the importance of these issues and reported that privacy, followed by access and accuracy and lastly property was the order of importance of these issues in the framework and therefore, confirmed the relevance of these four issues to cyberethics.

6. Conclusion and recommendations

Use of technology by doctoral students facilitates searching and retrieval of information needed for their academic endeavors and consequently, the

successful completion of their doctoral programmes. The need to be aware and knowledgeable on ethics surrounding the use of ICT is therefore, important. LIS doctoral students are aware and possess knowledge about cyberethics and have adhered to all the four issues in the PAPA framework (property, accuracy, privacy and access). The PAPA framework adopted for the study is common in the consideration of cyberethics. However, it is recommended that cyberethics education should be provided to these students by librarians to enable continuous adherence to cyberethics during their programme and after graduation.

7. References

1. Abubakar, D. and Adetimirin, A. (2015). Influence of Computer Literacy on Postgraduates' Use of E-Resources in Nigerian University Libraries. *Library Philosophy and Practice*. Paper 1207. Retrieved on October 26, 2016, from: http://digitalcommons.unl.edu/libphilprac/1207.
2. Akbulut, Y., Uysal, Ö., Odabasi, H. F. and Kuzu, A. (2008). Influence of gender, program of study and PC experience on unethical computer using behaviors of Turkish undergraduate students. *Computers and Education*, 51(2): 485–492.
3. Beycioglu, K. (2009). A cyberphilosophical issue in education: Unethical computer using behavior-the case of prospective teachers. *Computers and Education*, 53(2): 201–208.
4. Conger, S., Loch, K. D. and Helft, B. L. (1995). Ethics and information technology use: a factor analysis of attitudes to computer use. *Information Systems Journal*, 5: 161-184.
5. Harris, A. L. (2000). IS ethical attitudes among college students: A comparative study. In The Proceedings of the Information Systems Education Conference 2008, 25: 801-807, Philadelphia, PA.
6. Igwe, K. N., and Ibegwam, A. (2014). Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria. *International Journal of ICT and Management*, 2(2): 102-113.
7. IKeepSafe (2014). Cyber ethics. Retrieved December 20, 2016 from:http://www.ikeepsafe.org/educators_old/mor e/c3-matrix/cyberethics/.

8. Ismail, A., Abiddinn N. Z., and Hassan, A. (2011). Improving the Development of Postgraduate Research and Supervision. *International Education Studies*, 4(1). Retrieved on January 15, 2016 from www.ccsenet.org/ies.
9. Johnson, D., and Simpson, C. (2005). Are you the ©opy cop? *Learning and Leading with Technology*, 323(7): 14–20.
10. Ki, H., and Ahn, S. (2006). A study on the methodology of information ethics education in youth. *InternationalJournal of Computer Science and Network Security,* 6(6): 91–100.
11. Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 10(1): 512.
12. Onyancha, O. B., (2015). An informetrics view of the relationship between internet ethics, computer ethics and cyberethics. *Library Hi Tech*, 33(3): 387 – 408.
13. Özer, N., Uğurlu, C.T., and Beycioglu, K. (2011). Computer teachers' Attitudes toward Ethical use of computers in Elementary Schools. *International Journal of Cyber Ethics in Education*, 1(2): 15-24.
14. Peslak, A. (2006). PAPA revisited: A current empirical study of the Mason framework. *Journal of Computer Information Systems*, 46(3): 117-123.
15. Rama, S. (2014). Panoramic View of Cyber Ethics. *IITM Journal of management and IT*, 5(1): 56- 62.
16. Ramadhan, A., Sensuse, D.I., and Arymurthy, A.M. (2011). E-government ethics: a synergy of computer ethics, information ethics, and cyber ethics. *International Journal of Advanced Computer Science and Applications*, 2(8): 82–86.
17. Sinha, M. K., Singha, G., and Sinha, B., (2011). Usage of electronic resources available under UGC-INFONET digital library consortium by Assan University library users. International CALIBER. Goa University, Goa. Retrieved on June, 18 2016, from http://www.shodhganga.inflibnet.ac.in/dxml/bitstream/handle/1944/164/50.pdf.
18. Supavai, E. (2014). Measuring online moral reasoning: The development and psychometric properties of the cyberethics scale. A dissertation submitted to Boston University.

19. Swamy, P., and Kishore, K. (2013). Use of e-resources by postgraduate students of the institute for financial management and research (IFMR), Chennai, India. *ELibrary Science Research Journal*, 1(12). Retrieved on September 21, 2016 from Isrj.in/uploadedArticles/133.pdf.
20. Woodward, B., Martin, T., and Imboden, T. (2010). Expanding and Validation of the PAPA Framework. Information Systems Educators Conference (ISECON) Proceedings, 27(1321). Nashville Tennessee, USA. Retrieved on November, 12, 2016 from www.aitp-edsig.org /proc.isecon.org.

The Ethical and Quality Implications of Legal Education in Kenya

by Daniel W. Muthee[1] & Elizabeth W. Wambiri[2]

1. Introduction

The history of legal education in Kenya traces back to the genesis of the first university in Kenya. Previously, training of legal professionals took place in the University of Dar es salaam or other parts of the world such as India and Britain. At the eve of Independence, the government converted the previous Royal College into the University of Nairobi. It is here that the first Legal education (LE) in Kenya took place. It has since expanded to other public and private tertiary institutions within the country.

From a glimpse, LE in Kenya has been a success story for many years. The first LE was taught by top notch scholars from all over the world and admitted the best brains fondly referred to as the crème of the society. Consequently, LE has achieved a lot of milestones such as prudent management of the law schools, production of high caliber top notch legal scholars and minds, maintenance of ethical standards and values. The dress code is one ethical and professional code the legal training has maintained over the years. Another milestone has been the exponential students' enrollment in legal studies as well as the opening of several law institutions in the country. This is the hall mark of an admirable career and role modeling.

This notwithstanding, ethical and quality issues and implications have been serious contestations particularly when there is exponential student enrollment. The questions of sustainability of ethical and quality standards amidst high student enrollment, spiraling budgetary constraints and inadequate trainers is of major concern.

The exponential students' enrollment in the law schools is an inevitable fact. The government's desire is to open up more training opportunities for

1 Department of Library & Information Science
2 Law School, Kenyatta University

all qualified students. This is at the background of massive enrollments at primary schools and secondary schools which was occasioned by the Free Primary (FPE) and Free Day Secondary School Education (FDSE). Somehow, the high enrollment is a resultant of the high enrollments at the pre university and pre tertiary levels of education and it is on this premise that the government has opened up massive training at tertiary institutions. Currently, there are several institutions offering legal education in Kenya up from the former University of Nairobi and Moi University. The new institutions offering legal education are Kenyatta University, Mt. Kenya University, Catholic University of Eastern Africa (CUEA), Jomo Kenyatta University of Agriculture and Technology (JKUAT), Kenya School of Law and the far flung universities of Jaramogi Oginga Odinga and Kisii. The expanded training opportunities in legal education have had its own share of challenges.

Among the key challenges identified is budgetary constraints and building staff capacity to deal with the challenges. The government has made critical strides particularly in supporting students from poor socio economic backgrounds, special needs, regional and gender disparities. Without such a strong proactive and affirmative support, it would be impossible for students with poor background to study legal education. Legal education is expensive and costly. All the institutions offering legal education with exemption of University of Nairobi have no hostels and even so, the hostels in the University of Nairobi are not enough for the unprecedented high enrollment.

However, there is still very high demand for legal studies in the country. Population in Kenya now stands at 44,000,000 people and the ratio of the population per lawyer is still very low. This has given the universities strong impetus to for higher institutions to start legal studies, albeit with sub standard infrastructure and poorly trained legal trainers. The focus is on raising students' numbers as a source of revenue for bridging the serious budget gaps from dwindling government allocations. This in the process also leads to disregard for the legal studies as a highly intellectual engagement that requires highest qualifications. They end up going for the minimum qualifications as long as the students can pay.

What therefore seems to emerge is that there is serious ethical and quality issues and implications in the provision of legal education. It is against

this background that the paper focuses on interrogating the ethical and quality implications as derived from training of LE.

2. Background information

The expansive growth of university education in Kenya is meant to address the previous low transition rate from secondary school into tertiary institutions (Republic of Kenya, 2005). It is a catapult to deal with massive numbers of students transitioning into secondary schools and eventually into universities and other tertiary institutions. The chickens have come home to roost with the completion of the primary and secondary cycle for the free primary education (FPE) and Free Day Secondary School (FDSE). The FPE has had a strong trigger effect on training needs in Kenya. The government was at a crossroads when the big enrollment triggered by FPE transitioned into secondary schools. The FDSE also ushered a large transition rate into tertiary institutions. Though the FPE and FDSE started as political exigencies and expediencies, the initiatives had widespread ethical and quality ramifications (Ohba, 2009). The efforts are the justifiable as they in a way tried to bridge the inequitable access to legal studies (formerly an area select few). It however, bled pockets of unethical practices in an effort to increase numbers and to compete with others. This slowly ended up as the sacrificial alter of quality training (Oketch and Ngware, 2013; Brookings Institution, 2013).

The Kenyan government has put up significant strategies to expand legal education in pursuant of the National philosophy, vision and mission of the Kenya government (Republic of Kenya, 2012). The philosophy guides and directs the ideals of the Ministry of Education. Human and economic development is critical in the growth of a nation since it puts the country on a vintage and significant higher pedestal for a long time. LE is expected to instill knowledge and lifelong skills particularly in the country's jurisprudence and justice systems (Republic of Kenya, 2013; United Nations, 2013).

A preview of relevant international conventions and protocols shows Kenya is a signatory to conventions and protocols which emphasize a holistic training and quality education. The acceptance of holistic education implies acceptance and recognition of multidisciplinary societal values that encompass issues such as honesty, tolerance, mutual respect, equality of human beings, peaceful coexistence and hard work (Odhiambo, 2012; Re-

public of Kenya, 2012; United Nations 2013). These are the ultimate goals expected of LE.

Sample studies on implementation of FPE and FDSE indicated several challenges. The challenges faced had a trickledown effect on training and teaching of other programs in the tertiary institutions such as universities and other institutes of higher learning. The trickledown effect was notably heaviest in programs such as the training of legal studies, medicine and science. The approach in teaching and training these courses is requires high precision and greater adherence to ethical standards and quality maintenance. That is why challenges were significantly noted in the implementation of the different phases of the FPE, FDSE and eventually university education. Though university education is not free as such in Kenya, the students admitted under the defunct Joint Admissions Board or the current Kenya Universities and Colleges Central Placement service (KUCCPS) pay minimal amount as compared to module two students. They precisely pay fewer fees annually than they would pay in one term in secondary schools (Republic of Kenya, 2005; UNESCO 2005). The university fees were introduced in 1995 as an education cost sharing measure between the government and the students/parents. This explains why the fees have remained the same since 1995 (twenty years down the line) despite high inflation rates. Apparently, the low fees by KUCCPS students have brought the unstated preference for the module two students since they pay high fees. The universities and colleges teaching highly specialized courses such as law and medicine silently opts for as many as possible students in module two. This is because they help the universities and colleges meet the deficit from the government

A UNESCO study in 2005 and subsequent study in 2010 identified myriad challenges in teaching of several programs in primary and secondary schools as well as tertiary institutions. The identified challenges include challenges associated with massive student enrollment. Among these identified challenges are unproportional trainer student ratios, inadequate trainers and lecturers against increased responsibilities for the staff, inadequate physical resources and teaching materials. Others are low and poor students entry behavior as well as low motivation for both staff and students. All these challenges are despite the several milestones the country has made in improving quality, equity and ethical standards (Republic of Kenya, 2013).

Ethical standards and quality education is the base line for sustainable socio-economic and political developments. Equity, ethics and quality in education is the core of professionalism and career growth. This is what should define LE and increased access to LE should be defined along ethical and quality standards (Republic of Kenya/UNESCO, 2012).

Promotion of ethical culture and enhancement of quality service and products throughout the worlds is the basis for ability to operate and sell products and services throughout the world. LE is a global commodity. Whatever values and ethical considerations are in one country applies to the rest of the countries. This means that increased student enrollment and constraints in budgetary allocations should not mean low quality products and negligent on otherwise valued ethical norms particularly in teaching, researching and training in LE. LE is the hallmark of sustainable justice and governance systems throughout the world. The emphasis on ethical values and quality service and products in LE is of utmost important in developing countries whose governance and justice systems are pretty young and at the nascent stages.

3. Theoretical framework

This paper is anchored on the capital theory according to Hargreaves (2001). Hargreaves Theory emphasizes on effectiveness and improvement in schooling. Definitely, knowledge and skills acquisition as well as ethical values and enhancement of quality service to humanity are part of the effectiveness and improvement in schooling Hargreaves espouses. According to Hargreaves, cognitive and moral values build a sound intellectual base. It is upon the intellectual base that moral societies and communities spring from. The proverbial oral narratives all talked all had moral lessons to teach and to pass to the world and societies so that the world could prosper, harness its resources well, share equitably whatever was available and dispense justice fairly and wisely. This is what capital advocates and envisages in LE.

All societies from time immemorial have passed down to the future generations moral values that spell societal expectations. These are universal values but as much as they are universal, certain disciplines have certain ethical values associated with them. For instance, teachers are expected to hold the highest moral values as role models to the students they teach and

spend a lot of time with. Professionals involved in LE are equally expected to hold highest ethical values in cognizance of their roles as part of the much respected world judicial systems. Unfortunately, these ethical standards and quality expectations are not automatic. They have to be nurtured, cultivated and promoted through effective schooling systems and continuous improvements. Quality service is a daily experience that involves continues struggles towards better service and products coupled with ethical expectations. They have to be safeguarded through effective structures and frameworks such as performance appraisals, benchmarks, regulatory bodies dealing with maintenance of standards, professional codes of conduct safety and occupational standards among many others. These are difficult systems to maintain if they are not well safeguarded and policed. This is why Hargreaves talks of effectiveness and improvement in schooling if societies are to gain maximally in social capital. Years of effective schooling in ethics and quality service yields valuable moral values such as honesty, faithfulness, loyalty, honesty, patience, and love for mankind, peace, hard work and respect for others among many others. This theory is therefore appropriate in this paper since it propagates the need to enhance schooling of ethical values and considerations in the teaching and training of LE.

4. Statement of the problem

Kenya has registered high student enrollment for the last ten years since the inception of FP, FDSE and the inevitable expanded universities and colleges training programs. This expansion in training programs has had its own share of challenges.

First, training in LE has had ethical and quality challenges. Law is about dispensing justice. There is temptation to tamper with justice in societies as has been witnessed over the years. Tampering with justice is both unethical and inequality. The LE lays foundation for the quality of legal professionals that will be charged with the justice systems.

In Kenya, there has been a big upsurge in student enrollment in law schools. This is despite the increase in the law schools form the traditional two schools to ten schools. The increase is inevitable considering that the law schools have grown deep appetite for money from the lucrative module two students. As earlier argued, the module two students pay more fees and enable the law schools to curb the deficit in budgetary allocations. This

notwithstanding, the ethical and quality sustenance challenges are insurmountable. The issues of overworked and demoralized staff, ill prepared staff, admission of students with low intellectual capacity to pursue strenuous LE course, temptations to have short cuts by students and staff are rampant. It is against this background that the paper has attempted to look at the expected ethical and quality implications in dealing with LE and particularly in the face of inevitable widespread expansion of LE.

5. Purpose and objectives

The purpose of this paper is to assess the implications of current teaching and training of LE in Kenyan legal schools. The paper is concerned with the question whether training of LE in Kenya is in tandem with the expected ethical norms and quality standards? The paper revolves around two objectives: To assess the management strategies and profile the current trends in training and teaching of LE in Kenya; to examine the emerging trends.

6. Research methodology

The paper employed mixed method research design. It involved both quantitative and qualitative data generated form primary sources of data such as interviews with purposely selected sample of twenty trainers and trainees in LE. The interviews were instrumental in pinpointing the emerging trends and challenges. The study also employed secondary sources that included review of government documents and institutional policies and documents. Literature review from secondary sources was done so as to give the study the background and impetus it needed.

The respondents were both trainers and trainees in LE and were drawn from the University of Nairobi, Kenyatta and Mt. Kenya Universities. The study left out trainers and trainees from Moi, Kisii, Jomo Kenyatta University of Agriculture and Technology (JKUAT) Nazarine, Catholic University of Eastern Africa (CUEA) and Kenya School of law due to time limitations.

7. Results and discussions

The study sampled twenty respondents. The data was collected through interviews and simple questionnaires requiring the respondents to list the

challenges encountered and emerging trends in training and teaching of LE according to their observations. The data was collected as follows:

Table 1: Distribution of respondents by legal schools/universities

Legal school/university	No. of respondents	%
University of Nairobi (Parklands Campus)	8	40
Kenyatta University (Parklands Campus)	7	35
Mt. Kenya University (Parklands Campus)	5	25

One notable aspect is that the three legal schools under study are all based in the parklands neighborhood in Nairobi city. The strong coincidence is a result of the amenities associated with Parklands. Parklands is a high end neighborhood. The inhabitants are mostly middle or upper middle income earners of Asian and African descent. The neighborhood is well connected with good road networks to and from all directions of the city. Prospective students for legal studies would easily assess the campuses either driving or by public means.

Current management strategies for legal education and emerging trends

The study noted several management strategies and current trends associated with training and teaching of LE in Kenya. Among the key management strategies and trends noted are:

1. Enhancement of student enrollment particularly module two students. The motivation is to bridge the existing gap in budgetary constraints. Most of the institutions offering LE are heavily underfunded despite the need for expensive reading and physical resources. Other resources are dilapidated due to continuous use over the years. This was noted in the University of Nairobi which is a fairly old legal studies campus. Kenyatta University is a relatively young legal education school which was accredited by the CUE in 2014 while Mt. Kenya is yet to be accredited. Accreditation requires up-to-date resources, observance of the highest ethical standards and quality education as epitomized through continuous improvement of resources since accreditation is a continuous process. Continuous improvement means availing the best and most recent resources, meeting the required

ethical standards, improvement of staff capacity and benchmarking with the best LE schools.

2. Improvement of staff capacity is a key management strategy. All the institutions studied had staff development programs for the teaching staff. The staffs under staff development are supposed to engage in their pursuit for higher educational qualifications as they work. This is in an effort to continuously improve the capacity and quality of their staff. It was noted that some of LE schools lacked staff that were proportional to the number of students. In such cases, the schools depend on adjunct staffs that practice in law firms in an effort to curb the serious disproportional staff levels.
3. Judicial attachments and internships are key management strategies identified. Apart from the usual pupilage, the students undergo two judicial attachments in their 2nd and 3rd years. This is a management strategy of preparing them for the market and enabling them to have a niche over other similarly trained graduates. The study noted that while judicial field works are important activities that improve the quality of training and teaching LE, they were infrequent. This could only be attributed to cost cutting endeavors. Unlike judicial attachments and internships where students are financially responsible, the legal schools are responsible for field trips and therefore, the reasons for the cost cutting measures.
4. The promotion of Information Communication Technologies (ICTs) in the training and teaching of the LE has ensured quality education. In addition, it has ensured the availability of several online e-books and journals which would not have been available under normal circumstances.
5. Systematic monitoring and evaluation of adherence to ethical values and maintenance of quality standards. All the campuses studied are ISO certified. ISO certification requires maintenance of professional ethics and continuous improvement in all spheres of life. The study noted deliberate efforts to maintain proper records such as class attendance, complaints and compliments register.
6. In an effort to achieve international recognition, it was noted that the LE schools were all ranked in the world web metrics. For one to at-

tain good ranking, the individual institution aspires to adhere to the stipulated standard ethical norms and maintain a strong flow in the continuous improvement path. The philosophy underlying continuous improvement is based on the fact that there is no end to improvement particularly in the face of new challenges emerging daily. The study identified the following unethical challenges shown in table 2 below and which could affect negatively the quality of LE in Kenya:

Table 2: Factors affecting ethical and quality LE

N=20

Challenges identified	No. of responses	%
Staff and student absenteeism	8	40
Poor syllabus coverage	7	35
Proliferation of legal schools with inadequate resources	5	25
High student enrollment	11	55
Inadequate teaching and learning resources	5	25
Ill prepared trainers/under qualified trainers	4	20
Poor regulatory frameworks	5	25
Low student/staff perception	6	30
Inadequate supervision/monitoring and evaluation	4	20
Budgetary constraints	5	25
Quality of students admitted	4	30

High student enrollment (55%) was noted as one of the leading causes of unethical practices, poor quality service and ill prepared graduates.

8. Conclusion and recommendations

This paper has discussed the genesis of LE in Kenya and its exponential growth amidst a lot of challenges. It has discussed a plethora of unmet ethical and quality issues in provision of LE. Despite these challenges, it was noted that Kenya has produced some of the finest legal minds and scholars

in the region and the world over. Among the challenges identified is the massive student enrollment which has tended to spiral over the ethical and quality issues gained. This could be contained through a systematic student enrollment that oversees a proportionate teacher student enrollment. It could also be contained through a sustained and serious staff development program. Such an aggressive staff development could easily contain the high student enrollment coupled with aggressive infrastructural staff development.

Other challenges such as staff absenteeism and poor syllabus coverage could easily be dealt with through aggressive monitoring and evaluation system as well as constant student feedback. The cumulative effect of such challenges if unchecked could adversely affect the envisaged ethical and quality LE in Kenya.

9. References

1. Brookings Institutions. 2013. Towards universal learning: What every child should learn. Brooks. Brunner, J.S. 1961. The Act of Discovery. Harvard Educational Review, vol. no. 31, 1961.
2. Odhiambo. 2010. Task force on realignment of education to the constitution 2010 and vision 2030 and beyond. The Government of Kenya.
3. Republic of Kenya. 2005b. Kenya Education Sector Support Program 2005-2010: Delivering Quality Education and Training to all Kenyans. Nairobi: MOEST.
4. Republic of Kenya 2007a. Gender and Education Policy in Kenya. Government Printer. Nairobi.
5. Republic of Kenya 2007b. Harmonization of the Legal Framework on Education Training and Research: A report of the task force on review and harmonization of the legal framework on education, training and research.
6. Republic of Kenya 2010a. The Constitution of Kenya, 2010. The Attorney General. Nairobi.
7. Republic of Kenya 2012 a. Sessional paper No 14 of 2012 on realigning education and training to the Constitution of Kenya 2010 and Vision 2030 and beyond. Ministry of Science and Technology. Nairobi. Kenya

8. Republic of Kenya 2012b. A policy framework for realigning education to the constitution 2010 and vision 2030 and beyond.
9. Republic of Kenya. 2005a.Sessional Paper No 1 on policy reforms for education, training and research: Meeting the Challenges of Education, training and research and in the 21st Century. Ministry of Education, Science and Technology (MOEST) Nairobi.
10. Republic of Kenya/UNICEF 2012. Education for all (EFA) End of decade Assessment (2001-2010). Ministry of Education and UNICEF. Nairobi.
11. UNESCO 2004a. Monitoring Report 2005 through the UNESCO International Bureau of Education, Geneva. Anderson, L. W. 2004. Increasing Teacher Effectiveness. 2nd ed. Paris, UNESCO International Institute for Educational Planning.
12. UNESCO 2005b. EFA Global Monitoring report 2005: Education for all, The Quality Imperative, UNESCO, Paris.