Profiling and manipulating human behaviour: a core contemporary privacy concern.

Alan Mckenna

"The more a man may live according to his own inclinations, the more he is free." (Peter Forsskål – Thoughts on Civil Liberty: 1759).

1. Introduction

A feature of recent years has been the almost incessant stream of privacy related stories that have been reported by both traditional media and new media sources, with rarely a week going by without at least one new privacy related story emerging. Such stories arguably either individually or cumulatively add to the perception that the current era appears to be one in which privacy violations, or potential violations, are endemic, with our private lives and personal information being beset by a plethora of watching eyes, be they physical, mechanical or digital.

With such concerns over privacy violations what are the specific harms that emanate from such intrusions into our personal lives? With so much written about potential or actual privacy violations, at times it appears almost taken for granted that this is a negative thing and as such there is perhaps no need to elaborate further as to the specific harms we might face when our privacy is violated. Indeed, one American journalist recently wrote how after years of trying to protect his privacy, he is now literally going to go with the information flow and abandon his attempts to protect his online privacy as it could be that the benefits of doing so may outweigh any downside. (Hill, 2011). Perhaps Hill's conversion can in some ways be seen to reflect a new culture that is developing with the proliferation of information and communication technology (ICT) devices, and how we communicate and inform others about our lives. Anyone who travels on a train in the UK today for instance will listen to a varied number of telephone conversations during their journey, in which the speakers provide without any apparent concern, all types of personal information. Travel back in time twenty years, and the same passenger would witness their fellow passengers talking in mostly hushed tones to each other, providing little clue as to what they were talking about.

Privacy arguably however remains fundamentally important and will continue to do so despite how the new technologies have given us the possibility to communicate and share information more readily, with one commentator arguing its importance can be seen as lying in Man's DNA itself, for paradoxically whilst we are social beings who like the company of others and are inquisitive to know what are fellow humans are doing, we also like our own private space, feeling inner security in being able to go home and draw the curtains on the world. (Melville-Brown, 2008). As such of course it can be said that a fundamental feature of

the human form is our right to personal autonomy. In their famous paper on the right to privacy, Samuel Warren and Louis Brandeis, refer to American Judge Cooley's phrase, 'The right to be let alone'. (Warren & Brandeis, 1890). This phrase perhaps provides us with an underlying essence of why privacy matters. Not just with the guaranteeing of our personal autonomy in respect of for example being able to withdraw from the world and its gaze at our choosing, but more than this, in not having our lives in ways we have little or no control over, directly interfered with by others, whether they be individuals, corporations, or states, when they obtain and use information specific to us. In 1960 the American academic, William Prosser, identified four distinct ways in which he considered personal privacy could be infringed: (i) by intrusion upon a person's seclusion or solitude, or into his private affairs; (ii) by public disclosure of embarrassing private facts about a person; (iii) by publicity which places a person in a false light in the public eye; and (iv) by appropriation, for the defendants advantage, of a person's name or likeness. (Prosser, 1960).

Unsurprisingly it has been argued that Prosser's understanding and interpretation of privacy violations, in coming from a pre-digital age, are insufficient for today's world, in that digital technology has clearly extended the situations and forms by which personal privacy can be violated. (Keats Citron, 2010).

What this paper seeks to consider is that in looking at the changing developments relating to the potential privacy implications that the advent of digital technology has brought about, the possibility of the carrying out of highly sophisticated profiling of individuals now exists, and as a consequence of such profiling possibilities it may be argued that it is not only potentially feasible to predict human behavioural patterns by use of the information obtained, but to actually take the next step and in theory manipulate human behaviour. In looking to address such issues, whilst to date the primary focus of attention in respect of one particular use of such profiling techniques relates to behavioural advertising in the online world by commercial organisations, it is important to be aware that although such practices are being used from the commercial context of being able to sell more goods and services, without doubt the privacy invasive technologies being utilised can be used by other types of parties, most obviously governments and related governmental organisations for alternative purposes, and like commercial operators their aim would be to induce change in individuals behaviour.

In looking at how such challenges have to date been addressed and how they might be met in the future, it is necessary to consider the full range of protective provisions, be they regulatory, technical or for example educational, as arguably ultimately no one single protective course will by itself be sufficient to counter the challenges faced. Naturally the primary focus has been on regulatory provisions, and from a global perspective Europe has been at the forefront of much of the analysis and regulatory development that has taken place in seeking to address the new privacy related challenges that have emerged. It is perhaps unsurprising and appropriate that the very first data protection law created anywhere in the world came from within Germany, when in 1970 the German state of Hesse sought to address concerns that had emerged over the surveillance implications for the citizens of Hesse, whose sensitive personal data was being collected and stored on public databanks. (Simitis, 2010) (Burkert, 1999). It is appropriate of course that such legislative leadership should emerge

from Germany when we reflect on how the Nazi regime had used detailed information collection systems to help facilitate control and mass murder.

Reflecting a general trend of growing global interconnectedness in terms of not only communication links, but also of general reliance, there have been calls for comprehensive global privacy instruments to be developed and adopted in order to protect individuals privacy. (International Data Commissioners, 2009). Whether agreement could be reached on a binding comprehensive instrument that is fully enforceable throughout the world would seem currently a difficult prospect.

Whilst much of what will be discussed concerns the use by commercial operators of personal information, the role of the state as already alluded to requires close consideration, and despite the positive recent example of the use being made of information and communication technologies in the form of social media to help facilitate the protests that led to the collapse of a number of despotic regimes, undoubtedly states whether they be undemocratic and democratic in nature, will develop their understandings of the new technological systems and potentially utilise them in ways that could ultimately inhibit personal rights and freedoms, and this is something which we must be acutely aware of and be prepared for.

2. The developing use of profiling within the context of a growing information dependent society

For more than twenty years western governments have been keen to locate the development, collection and usage of digital information at the heart of their policy agendas, with an overarching aim being the creation of what has variously been labelled an Information Society, Knowledge Society or Digital Economy. Whilst recognising the importance in part of the social aspects of such development, much of the primary focus has concerned the economic potential of using the new technologies and digital information. This can of course at times lead to problematic conflicts occurring between the aim of facilitating the creation of economic wealth and economic development, in contrast to other more societal specific goals and values. We should perhaps locate our discussion within this context, with tensions between such issues intensifying in times of general economic difficulty.

The notion of profiling can be seen to occur in a wide variety of contexts in modern life, and arguably Man has in fact engaged in acts of profiling since his/her first emergence, profiling both his/her fellow humans and the environment in which he/she exists. At its heart the aim of profiling may be said to be the obtaining of information and knowledge.

In a modern context Hildebrandt considers that profiling can be seen as:

‘The process of ‘discovering’ correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to indentify a subject as a member of a group or category.’ (Hildebrandt 2008:19).

Of itself profiling arguably should neither be seen as bad nor for that matter good. (Gutwirth and De Hert 2008: 289). What is key however in assessing its nature is how it is carried out and for what purposes it is carried out. The knowledge that is generated by profiling Gutwirth and De Hert have termed non-representational, as the profiles are said not to be about representing a current state of affairs, but look rather to predict future behavioural characteristics based upon the past actions of the parties that are subject to the profiling. (Gutwirth and De Hert 2008: 289). On a general level the undertaking of surveillance activities, whether by companies or governments, in order to profile specific individuals or groups has been called social sorting, the essence of which is to classify individuals or groups according to varying criteria. Of course the sorting of populations is a common feature of modern life, with examples being sorting to decide who should be taxed at a particular rate, or who is eligible for a specific benefit. But whilst some forms of social sorting based upon profiling activities may be of fundamental importance in the effective running of a modern society, we must remain vigilant as some social sorting can be tantamount to discriminatory practice. (Ball et al 2006: 11.4).

With the use of information and communication technologies (ICT's), Van der Hof and Prins have described how what they consider to be a fundamental change has been taking place in the consumer marketplace, contrasting the early 20th century notion of mass production based upon similarities between consumers that led to limited choice, against the contemporary idea of mass individualisation, in that goods and services are now becoming tailored to the desires of consumers. In order to achieve what has been generally termed personalisation of service, companies use ICT's to select, filter and classify user information. (Van der Hof and Prins, 2008: 112-113). This may seem unproblematic, even perhaps clearly beneficial to the individual consumer, in that his/her desires are being specifically catered for. However, Van der Hof and Prins point to what they term the dark side of personalisation, raising a number of concerns over potentially detrimental impacts for both the individual and society in general. Of fundamental concern for them is the ultimate impact on individual autonomy, and whether personalisation can lead to discriminatory practices when such detailed information has been collected. (Van der Hof and Prins, 2008: 115-124). We can see a facet of personalisation with the emergence of individualised advertising. The growing development of ICT's have enabled commercial enterprises to develop a form of advertising that moves away from the traditional standard of a generalised advertising campaign, to one that targets individual's, based upon the information and knowledge that advertisers accumulate on individual consumers interests via profiling; this has become known as behavioural advertising, the provision of your own personal online adverts. It is quite noticeable and for some people probably quite alarming how adverts for products that you may have been looking at on one particular website, then appear persistently to follow you around the web, almost demanding your attention.

Attempts to use an individual's information and behavioural patterns should not be seen as unique to commercial enterprises, for it does not take too much imagination to envisage its use and development for governmental purposes. The influencing of behaviour by rulers/governments naturally has a very long history. State controlled violence is an obvious

extreme example of a long standing behaviour influencing mechanism. Today, governments in democratic states primarily rely upon legislation, taxation, and information provision in seeking to influence behaviour. However, there appears a growing recognition within governments that there are alternative strategies that could be employed which may be cheaper and potentially more effective. An example from the United Kingdom of such recognition came in 2004 when the UK Prime Minister's Strategy Unit undertook research into how government policy could be enhanced and public behaviour positively influenced by the use of sophisticated psychological techniques. (Prime Minister's Strategy Unit, 2004). A further report commissioned by the UK government was published in 2010. Its authors, The Institute for Government (IFG), in asking why it was necessary to consider alternatives to the traditional methods used to influence behaviour, argued that behavioural theory provided two reasons: firstly, that the impact of existing tools could be greatly enhanced by new evidence about how human behaviour is influenced; and secondly, because there were new and potentially more effective ways that 'government could shape behaviour.' (Institute for Government 2010: 8). Utilising the science of behaviour, the IFG argue that the acts of individuals are often influenced by sub-conscious cues. A technique they term Priming shows that individual's subsequent behaviour may be altered if they are exposed to certain sights, words or sensations. Thus, if people are pre-primed by cues they will behave differently. (Institute for Government 2010: 24). The IFG recognise that the techniques being considered may be utilised in a way in which individuals may not appreciate that their behaviour is being targeted and changed, or at least in how it is being changed. This could of course lead governments to face charges of manipulation. (Institute for Government 2010: 66). Consequently this would bring into play important issues such as infringement of personal autonomy, freedom of choice and control. Arguably, if such manipulative techniques are to be allowed to be used at all, then it would be appropriate if this occurred with the prior knowledgeable approval of those whose behaviour is to be targeted for change.

Use of new types of psychological techniques to influence behaviour clearly raise matters of fundamental importance, but it can be appreciated that governments when for example faced by a challenging financial environment, are likely to look for more effective and less costly ways to influence behaviour. Whilst all the ethical considerations involved may be outside the scope of the parameters of our discussion in this paper, what does bring the issue within its scope is if it can be argued that an individual's privacy is at risk of infringement by the use of such manipulative techniques. Thus for example, it may be asked whether our personal information is being used in a way that will facilitate the manipulation of our behaviour and is this ethically acceptable, both to the individual in question and to society as a whole?

In looking to achieve more effective use of such techniques, by effective I mean of course those that actually can be shown to change behaviour, with it being recognised that humans do not always respond in what may be seen as a rational way by doing unexpected things (Institute for Government 2010: 8), the likelihood is that it becomes important to adapt such techniques to meet individual personalities; and with the advent of advanced digital technology and profiling possibilities, this makes such effective use even more likely.

Reflecting genuine belief in its potential, following on from the IFG 2010 Report, the UK Government has now created within its Cabinet Office a seven strong Behavioural Insights Team, which includes academic experts on behavioural sciences. Cabinet Secretary, Sir Gus O'Donnell, who heads the team argues that, 'many of the most pressing public policy issues we face today are equally influenced by how we, as individuals, behave. We can all cite instances in which we know that we should act differently in our own self interest or in the wider interest, but for one reason or another do not. The traditional tools of Government have proven to be less successful in addressing these behavioural problems. The Behavioural Insights Team has been established...to help the UK Government develop and apply the lessons from behavioural economics and behavioural science to public policy making.' (O'Donnell, 2010). It should be noted that the UK is not alone in Europe in setting up such a unit, with the French Government also working on such projects. (Franco-British Council, 2010).

Whilst governments may be newcomers to the field, it would be extremely surprising not to find the advertising industry at the forefront of the field, as of course with the ceaseless pressures of the competitive commercial marketplace, advertisers and marketers will look for any advantage to put them ahead of their rivals. Historically, advertising has been conducted on what may be now considered as a rather random non-cost effective basis, in that the vast majority of people who encounter a particular advert are likely to have little or no interest in the advert and will not be influenced by its message. Now with the emergence of behavioural targeted advertising, on the basis of information collected directly targeted individuals are far more likely to be responsive to the specific adverts directed at them.

Understandably, it has been argued by legal academic Tal Zarsky, that a commonly used advertising model which sees optimal advertisements as being those which cross an individuals' barriers of perception, capturing their attention and affecting their comprehension, can be achieved with greater success in the online environment with content based upon personal data specifically tailored to individual characteristics detected via profiling techniques. The crossing of an individual's barriers of perception implies that the relevant message enters that individual's sensory register. In a similar way to what was discussed in terms of the technique of Priming, here the preferred form of perception refers to the shapes, colours and sounds which are optimally received by the specific individual. Being able to capture an individual's attention requires information to be obtained as to that individual's interests and on gaining access to their attention, the final task is to cause that person to comprehend a specific point, which naturally would be that they should consider buying a particular product. (Zarsky 2006: 216-217). An effective message from an advertisers' perspective could at times mean an unfair and manipulative message from that of its recipients. Again of course we run straight into questions of fairness and infringement of personal autonomy. (Zarsky 2006: 219). Where it might be asked is the boundary to be drawn between what is a fair attempt to influence and activities which are to be considered unfair and manipulative? (Zarsky 2006: 220). In contrasting the changing advertising landscape, it is argued by Lessig that there is likely to be general scepticism about the power of general television advertising to control people's desires, as the motives are so clear. But he questions

what happens when the motives are not so clear cut, when a system appears to know what you want better and earlier than you do, how is it possible to know where the desires really emanate from? (Lessig, 1999: 154).

It is Zarksy's belief that the key to mitigating potential consumer detriment caused by personal profile constructed advertising messages, should be based upon two notions: firstly, by providing consumers with notice as to the tailoring of such individualised communications, and how their personal information is used to achieve this; and secondly, by assuring that consumers receive a balanced mix of messages. (Zarsky 2006: 221). Whilst providing notice to consumers of tailored advertising appears an appropriate solution, it should be asked whether mere notice of such advertising is potentially insufficient, and that for consumers to have a real appreciation of what is taking place they would need to be clearly made aware of precisely what is taking place. (Office of Fair Trading, 2010: 52). A pan European self-regulatory initiative for online behavioural advertising has just been launched. This is said to seek to enhance transparency and consumer control, enabling the consumer by clicking on a standard form and strategically placed Icon they will be provided with further information about behavioural advertising and the way they can manage their information preferences. (Internet Advertising Bureau, 2011). An additional suggestion that might be added when consumers click on the Icon, is providing the option of seeing a short film on the nature of the advertising that is being encountered, as this may prove far more illuminating in explaining the precise nature of the advertising that is taking place.

3. Profiling Technologies

If anything is certain about the technologies that can be used for surveillance and profiling purposes it is that they are going to become ever more pervasive and powerful, as clearly technological development is not going to stand still.

One of the key technologies that enable online profiling and behavioural advertising to take place, and which have continued to evolve since they first appeared are cookies. Cookies are text files which are placed on a user's machine by a web server, enabling the server to recognise a particular visitor to their website when they return to the site, this being considered of particular importance in respect of online transactions where ongoing steps need to be undertaken and the server needs to be aware of previous actions.

When studies found that over 30% of users were deleting cookies from their machines each month, this finding proved problematic for advertisers, as it meant that consequentially there was an overestimation of the number of true unique visitors to websites, with subsequent overpayment being made by advertisers to websites. As a consequence and desiring greater tracking reliability the advertisers sought new solutions. (Soltani et al, 2009). What resulted were far more powerful privacy intrusive cookies being developed. These newer forms of cookies have been variously called supercookies, Flash cookies, evercookies or ubercookies, having far greater storage capacities than normal cookies; and being stored outside the browsers puts them outside of the user's browser control. They can be difficult to erase, and

some types actually have the capacity to regenerate deleted cookies. (Tirtea et al, 2011). Furthermore, such cookies have the capacity to follow and identify users across multiple different sites.

Highlighting how pervasive they have become, research carried out in 2009 on U.S. websites, found that 54 of the top 100 U.S. sites placed Flash cookies on users machines. On several of the sites it was found respawning was taking place via the Flash cookie; that is after the user deleted the HTTP standard cookie, it was actually being recreated by the Flash cookie. Another even more recent investigation carried out by the Wall Street Journal in the United States, found that some large U.S. websites were installing more than 100 tracking devices including cookies on visiting users machines. The 50 most popular U.S. websites were examined to measure the quantity and capabilities of the tracking devices, and it was found that the 50 sites installed a total of 3180 tracking files on the test computer. They discovered that some of the tracking files had the capacity to record an individual's online keystrokes and to then transmit the text back in order for it to be analysed for content, tone and clues as to an individual's social connections. (Angwin, J and McGinty, T, 2010).

For the purposes of profiling it is important to appreciate that whilst significant data can be obtained via the use of just one type of ICT, if such data can be combined with data obtained via other types of ICT's, this could significantly increase the potential strength and depth of the overall profile achieved. Another of the technologies that has drawn attention over its profiling possibilities is data mining, which in essence is via the use of algorithms a way by which large datasets can be analysed in order to extract previously unknown and potentially useful information. There are said to be two distinct approaches to data mining – descriptive data mining, the goal of which is to discover unknown relations between different data objects; and, predictive data mining, which aims to be able to make a prediction about events, so this might for example take the form of predicting whether an individual fits a previously established profile. (Schermer, 2011, pages 45-46).

Whilst data mining has been highlighted for concerns over its implications for personal privacy, a counter argument is that the technology by itself is not the problem, it is how it is utilised is the potential problem, and with the technology being of great value, there are concerns that privacy worries could impact upon its future development and use. Clifton et al argue that the negative association with privacy infringement is unfortunate in that with growing amounts of data being created by various bodies, such volumes of data instead of offering greater insights can actually hinder overall understanding, without there being the capacity in place to be able to condense and analyse it. Furthermore, in an overt attack on lack of government/ public finance for research into such fields, they raise the spectre of a consequential negative privacy impact due to what they claim could result, that researchers will turn to private money where there might be less concern over privacy, and also less information about data mining subsequently being made public with knock on privacy impacts. (Clifton et al, 2006, pages 191-193).

Schermer has argued that when it comes to data mining and profiling, especially when carried out via an automated process, data protection law does not provide adequate protection. It is

his belief that there exists a lack of co-operation between the data mining community and data protection community, and with the law being based primarily on ex ante protection, there is little by way of ex post protection mechanisms. As such he feels there is a need for greater ex ante screening of data mining applications for potential risks and ex post checking of results, as currently data mining is a black box process for outsiders. In looking to provide adequate protection the recent initiative of developing privacy by design has an important role to play, with for instance the creation of Privacy Preserving Data Mining (PPDM) algorithms being used to protect personal data. Schermer however feels additionally it is necessary that there also are put in place mechanisms to detect improper use of data mining and profiling in policymaking, which may take the form of an oversight committee made up of a mixed discipline cohort. (Schermer, 2011: pages 49-52).

Information for profiling purposes is also obtained from what we may term the physical world, as opposed to the digital online world, although clear crossovers can be seen to exist. In the physical world the most well-known and abundant technology that is used for profiling purposes are CCTV systems. The United Kingdom has the perhaps dubious reputation of currently possessing the most CCTV cameras of any country in the world. An early use for such cameras was to protect retail stores from shop lifting. The in-store security camera could however soon be joined by a far more powerful privacy intrusive off-shoot. The Chief Executive of U.S. shopping marketing company, Shopper Sciences provides an interesting glance into what may be a future feature of physical retailing when he argues, 'New technology can use digital cameras to record shopper reactions to in-store marketing. This gives marketers real-time feedback on how they are responding and interacting with displays. More than simple traffic and monitoring software, the next generation of in-store analysis tools tell us emotional and physiological responses as well. Digital analytics company Affectiva offers real-time emotional tracking that can actually measure facial responses, head movements, and even heart beat as shoppers interact with products, kiosks, and retail displays.' (Ross, page 9). A further example highlighting a growing interest in what may be called machine based visual intelligence, the United States Defense Advanced Research Projects Agency (DARPA), the Agency which began the research into what ultimately became the Internet, has this year begun a new project called Mind's Eye. The aim of the military project is to move past the current state of the art in machine vision technology in which a range of objects and their properties can be automatically recognised, to seek a machine capability that currently only exists in humans, the visual intelligence to actually understand and analyse a particular scene. (DARPA, 2011). It takes little imagination to see that if such technology is successfully developed that it is likely in some form to move from the field of military usage to be used in commercial contexts, with undoubted potential privacy implications.

Until now the most significant way in which traditional retail stores have obtained information about their customers shopping habits has been via the use of loyalty cards. Of course it must also be remembered that traditional retailers will also have an online presence potentially providing additional information about their customers. But Ross holds out the possibility of even more enticing information collection that traditional retailers may be able

to obtain when he poses the rhetorical question, 'What if you could get online style metrics in-store? How powerful it would be to identify and track individual shoppers throughout their shopping journey, just like we do online, giving them customized offers, discounts, and communications as they move throughout the store. And then to know where non-buyers went after leaving the store?' (Ross, page 2). The emergence of two further technologies, Radio Frequency Identification (RFID) and Global Positioning Systems (GPS) in combination with shoppers' smart phones, now allow retailers potentially to identify shoppers when they enter a shop. (Ross, page 8).

RFID and GPS technologies provide the additional dimension to profiling technologies in that they produce location based tracking information. Highlighting how potentially invasive the information obtained via GPS can be, Malte Spitz, a German politician recently discovered that over a six month period from August 2009 to February 2010, his mobile phone company T-Mobile via GPS technology had recorded his precise location more than 35,000 times. What many people do not realise is that every few seconds mobile phone companies determine the nearest mobile phone mast to their phone to ensure efficiently routed calls. (Cohan, 2011).

GPS and RFID technologies are seen to be complementary in enabling instantaneous identification of location and therefore the tracking of people, vehicles or goods, with GPS providing a more general location and RFID far more accurate one, but RFID being more restricted in terms of when tracking is possible than GPS currently. An RFID tag when it passes within range of a compatible RFID reader via use of radio signals will record the time and location. (Monmonier, 2006: 75-76). Much of the early use of RFID came in respect of general stock movement management systems, with no related privacy implications, but there has become a growing awareness that they can be used in situations where there certainly will be privacy implications – active tags inserted into goods that theoretically could be tracked to a persons home or wherever they might be; use in smart cards; passports; and potentially most privacy invasive of all, actually inserted into the human body. (Ball et al, 2006, 9.8).

Reflecting the growing use of RFID tags (it is estimated that in 2011 2.8 billion will be sold globally, a third of which will be in Europe), the European Commission has recently signed a voluntary agreement by which companies who sign up to the agreement commit themselves to carrying out a Privacy Risk Assessment (PIA) before they release the RFID product onto the marketplace. (European Commission Press Release, 2011). The Agreement establishes a specific Framework by which signatories will adhere in making their PIA. (European Commission, 2011). Included in the PIA, RFID operators must assess the risk of third parties being able to access personal data from the tags that come within the range of third party RFID readers. This was a particular concern where tags were used in the retail sector and are not deactivated when goods left the store. The recommendation allows a tag to remain active if the PIA concludes that the active tag does not represent a likely threat to privacy or the protection of personal data. The PIA is another example of privacy by design which has been advocated as an important element in the overall structure of providing effective privacy protection, but to date the primary focus has been on regulatory provision arguably. (Article 29 Working Party, WP 180)

4. The European Union regulatory structure for privacy protection

When considering the regulatory structure for the protection of privacy provided by the European Union (EU) an appropriate starting point is the recognition that the EU has within its Charter of Fundamental Rights included two specific privacy related rights, Article 7 providing for respect for private and family life, which mirrors Article 8 of the European Convention on Human Rights, and Article 8 which provides for the protection of personal data.

With the coming into force of the Lisbon Treaty in 2009, not only has the Charter of Fundamental Rights become binding on most member states, but additionally the Treaty of Rome which established the European Community was amended and renamed the Treaty on the Functioning of the European Union (TFEU); the renamed treaty includes Article 16 which replaces and expands upon the old Article 286, and it is hoped will give data protection within the EU new impetus. As the new legal basis for data protection in the EU, Article 16 is applicable to the processing of all personal data in the private and public sectors, including in the area of police and judicial co-operation and common foreign and security policy. (Article 29 Working Party: WP168, pages 5-9).

In looking at profiling and especially profiling carried out where behavioural advertising is being undertaken, both Directive 95/46/EC (Data Protection Directive) and Directive 2002/58/EC (e-Privacy Directive) as amended by Directive 2009/136/EC, are applicable. Directive 95/46 provides protection for individuals in respect of the processing of their personal data. Key elements are the interpretation of processing, which is given a wide scope under the Directive and includes for example collection, recording, storage and alteration, and what constitutes personal data, with article 2 defining personal data as any information relating to an identified or identifiable natural person. It is important to appreciate that a broad notion of what personal data can be considered to be is provided for by the Directive. (Article 29 Working Party, WP 136).

Recital 26 of the Directive provides important guidance on when a person might be considered identifiable from the information, stating, ‘account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person,’ and it continues, ‘the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.’ Thus, it would appear where data has been rendered anonymous so that an individual is no longer identifiable, and as well it is unlikely that the individual will be identified taking into account the means that are likely to be made reasonably by a data controller or third party, then the data will not be considered personal data coming within the scope of the Directive’s provisions. However, it is somewhat problematic to assess precisely what might be considered reasonably likely to happen, and each situation would need to be considered on its own facts. What is clear is that complete anonymisation of personal data in order to hide an individual’s identity has been shown recently to be if not a complete fallacy then certainly not

as secure or watertight as it was once considered to be in this regard. (Ohm, 2010: 1716-1722). With the emergence of powerful re-identification algorithms it is argued that de-identification techniques designed to provide privacy protection are badly flawed. (Narayanan & Shmatikov, 2010).

The e-Privacy Directive 2002/58 provides for the protection of privacy in respect of the processing of personal data in the electronic communications sector. Article 5 of the Directive seeks to ensure communications confidentiality by for example protecting against unauthorised listening, tapping or other forms of surveillance of communications over public communications networks or publicly available communications services. The recent amendment to Article 5(3) brings about a fundamental change in users privacy protection, in that the storing of information or the gaining of access to information already stored in the user or subscriber's terminal equipment will only be allowed with the user's prior consent, when they have been provided with clear and comprehensive information in accordance with Directive 95/46/EC of the purposes for the processing. The change introduced means that rather than the user having to opt out to prevent the processing of their personal data across communications networks, they will now need to specifically opt-in to allow such processing. It needs to be pointed out that the Article 5 provision does not prevent any technical storage or access which is required for the sole purpose of carrying out or facilitating the transmission of a communication over a network. The Article 5(3) provision applies to cookies, as tracking cookies are considered information which is stored on a user's equipment and the cookies are accessed by advertising network providers when a user visit's an advertising networks partner website. (Article 29 Working Party: WP 171, page 8). Thus, a user will now have to specifically approve the placing of cookies on to their machines.

The provisions of the amended e-Privacy Directive are required to be introduced into member states national law by the 25th May 2011. The changes brought about by the amended Article 5(3) appear from a UK perspective as somewhat problematic. At a time of substantial economic difficulties across Europe, there is a belief that the amended provision could act as a potential inhibitor of online economic activity, and as such would be unwelcome. A specific concern in respect of cookies is whether or not permission to place cookies on a user's machine would need to be obtained on every single occasion, and any consequential impact on internet use and commercial activity that consequently might occur. The UK Government do however believe that consent will not be required in every situation, providing the example of where a cookie is essential for a service requested by the user, as with cookie use for a website shopping basket. (Vaizey 2011). This belief is based upon their interpretation of Recital 66 of Directive 2009/136/EC, which they consider via the use of browser settings allows consumers to indicate consent to cookies. Recital 66 states, 'Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user.' The Recital continues, 'Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.' The UK government

intends to directly copy the amended Article 5(3) into UK law, making reference as well to Recital 66. Work it is currently undertaking with browser manufacturers it is hoped will produce a browser setting solution that meets the consent requirement. (Department for Culture, Media and Sport, 2011: 71-76). Doubts have however been raised over whether a browser based automatic consent mechanism will meet the Article 5(3) requirements, which the Article 29 Working Party consider is likely to happen in only very limited circumstances, as firstly, based upon the need for valid consent, a user cannot be deemed to have consented merely because they have used a browser which by default enables the collection of information. They argue, 'It is a fallacy to deem that on a general basis data subject inaction (he/she has not set the browser to refuse cookies) provides a clear and unambiguous indication of his/her wishes.' Secondly, they consider that for browser settings to be able to deliver informed consent, 'it should not be possible to "bypass" the choice made by the user in setting the browser'. This refers to the new generation of cookies that can be re-created after being deleted. Lastly, they consider that where the browser is set to receive cookies in bulk as a default, this implies that users are accepting processing without knowledge of the purposes or uses of the cookie, which in the circumstances cannot amount to valid consent. (Article 29 Working Party: WP 171, pages 13-14).

As regards the information that is needed to be provided to users concerning the purposes of processing under Article 5(3), the UK government support Icon based initiatives that are currently being developed, by which a user can click on an Icon to receive details of the processing that will occur. (Vaizey, 2011), (Department for Culture, Media and Sport, 2011: 74). The Article 29 Working Party consider in respect of behavioural advertising that the use of Icons to facilitate information provision to the user is a positive move forward, and they believe that the creation of a symbol with related messages would meet the need for consumers/users to be periodically reminded of the existence of targeted advertising taking place. (Article 29 Working Party: WP 171, page 18). Whilst it is to be welcomed that the use of Icons in order to help with the provision of information to users is now being developed, it is regretful that it has taken so long for their potential usefulness to be recognised, as indeed I recommended their use in this context some 10 years ago. (Mckenna, 2001: 349).

Reflecting the growing concerns over the impact of online advertising, the European Parliament have recently adopted a resolution which in respect of behavioural advertising and its affect on personal privacy makes several specific requests to the European Commission which call for action to be taken; these include developing educational material that explains how consumers can protect their privacy online, and requesting that the Commission as soon as possible require the insertion of the words 'behavioural advertisement' into online advertisements, with a window providing a basic explanation of behavioural advertising practice. A further interesting feature of the resolution comes in respect of hidden advertising. The Parliament condemns the developing online practice of so called hidden internet advertising, which occurs when comments posted on social network sites ostensibly by distinct autonomous individuals are in reality made as part of a co-ordinated campaign seeking to influence attitudes and behaviour. The Parliament is calling on the Commission to look at the Unfair Commercial Practices Directive (2005/29/EC) which relates solely to

business to consumer relationships, to consider whether it needs updating to meet such new challenges. (European Parliament, 2010). Article 5 of the Directive provides ‘A Commercial practice shall be unfair if..(b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed..’ Whether such manipulative behaviour can be considered to fall within the realm of privacy infringement is arguable, although such activities do seek to change behavioural patterns based upon potentially the interpretation of personal messages and information. Such manipulation in the online environment is not restricted to commercial operators, with it being recently reported that the United States military is developing software to manipulate social media sites by the creation of fake personas to influence internet discussions. (Fielding & Cobain, 2011).

It is clear that the European Commission believe Europe’s privacy laws still need updating further to meet new challenges faced in the digital age and as such proposals will be put forward this summer by the European Commission to update Directive 95/46. The EU Justice Commissioner Viviane Reding has recently provided some overarching guidance as to key areas of focus. In seeking to enhance the protection of an individual’s personal data, she considers that the individual rights should be built upon four pillars: (1) “The right to be forgotten” – in updating the rules in this regard to better protect online privacy, she is seeking to provide individuals the right, not just what she terms the “possibility”, (reflecting difficulties that can be encountered), to withdraw their consent to data processing. (2) “Transparency”. Reding argues, ‘Individuals must be informed about which data is collected and for what purposes.’ For her, individuals must know their rights, and all information concerning the protection of personal data must be given in a clear and intelligible way. (3) “Privacy by default”. A key interpretation of this is an overarching requirement that consent must be obtained in all situations where personal data is collected. (4) “Protection regardless of location”. It is proposed that no matter where in the world a service provider is located and the means they use to provide their service, homogenous privacy standards for European citizens should apply. Thus, any company that operates in the EU marketplace or in the online environment and who targets EU citizens would be expected to comply with EU privacy regulations. (Reding, 2011). This would prove a significant change, as currently under Directive 95/46 non-EU based data controllers who do not use equipment situated in the EU fall outside its scope. (Article 29 Working Party, WP 168, page 9). It has already been questioned whether such a provision in reality is feasible given its extra-territorial nature. (OUT-LAW, 2011).

5. Conclusion

With the reliance we now place on ICT’s, never before in human history has it been so easy as it is today to collect and collate so much information about individual people, enabling sophisticated profiling to take place, and providing the potential for surreptitious manipulation of human behaviour on a mass scale to occur. Clearly information and communications technologies will continue to be developed, becoming ever more

sophisticated, and potentially privacy invasive. In looking to provide protection against the varied forms in which privacy infringement may be seen to occur, regulatory provisions arguably no matter how strongly constructed, are by themselves insufficient to provide an adequate level of protection. Whilst regulation can lay down the ground rules which are meant to be adhered to, the penalties to be faced where infringement is discovered, and act as an inhibitor to infringing behaviour, ultimately they cannot by themselves be a total safeguard. What is required is an holistic approach that in addition to a strong regulatory framework, includes as well protection via the notions of privacy by design, privacy enhancing technologies, self regulatory initiatives, information provision in a variety of formats with a prime example the development of Icon based information provision, and last but certainly not least, consideration as to how to utilise general educational provision to enable users to look to protect themselves. However, what must be recognised is that even with such an holistic approach ultimately there is no full proof way of guaranteeing an individual's privacy, and never will be, and the best we can hope to achieve is to devise the strongest feasible protection strategy we can.

The concern raised in this paper is that with the collecting and profiling of personal information in whatever form, it may then be possible to use such data to manipulate human behaviour. This if taking place without the knowledge of the targeted individual is a clear infringement of personal autonomy, and equally from a societal perspective a worrying development. It may be asked whether such manipulative technique usage should always be seen in a negative light however? There have been concerns recently in Europe over teenage suicide. In seeking to protect vulnerable teenagers one potential approach utilising online digital technology could for example be based upon work carried out by a research team that looked at what information could be obtained by analysing keyboard typing patterns. The researchers believe that it is possible to identify when someone is under stress by using such analysis, and it could also be used to identify the onset of a condition such as Alzheimers. (Blincoe, 2010). If it were possible to identify a potential teenage suicide victim via such profiling or by using it in combination with other forms of profiling, would it then be unacceptable to attempt to use online manipulative behavioural psychology to try to change a teenager's immediate mood? Again it must be argued that it comes down to the issue of personal autonomy of the individual and the need for there to be awareness of what is happening. For whilst in such a situation as this there may be a clear humanitarian concern where do we draw the boundaries, and where do we stop?

References

Angwin, J and McGinty, T (2010), Sites Feed Personal Details to New Tracking Industry, Wall Street Journal, 30th July 2010.

Article 29 Working Party, The Future of Privacy, WP 168, December 2009.

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, June 2007.

Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, June 2010.

Article 29 Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, 11th February 2011.

Ball, K, Lyon, D, Murakami Wood, D, Norris, C and Raab, C (2006), A Report on the Surveillance Society, Surveillance Studies Network.

Blincoe, R (2010), Your keyboard knows that it's you and you're stressed. New Scientists 7th January 2010. Online at www.newscientist.com/article/dn18350-your-keyboard-knows-that-its-you-and-youre-stressed.html/ accessed 17.04.2011.

Burkert, H. (1999), Privacy – Data Protection: A German/European Perspective. Online at www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf/ accessed 07.04.2011.

Cohan, N (2011), Its Tracking Your Every Move and You May Not Even Know. New York Times, 26th March 2011.

Clifton, C, Mulligan, D & Ramarkrishnan, R (2006), Data Mining and Privacy: An Overview, in Strandburg, K and Stan Raicu, D (Eds), Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, Springer Science.

DARPA (2011), DARPA Kicks off Mind's Eye Program, January 4th 2011. Online at www.darpa.mil/NewsEvents/Releases/2011/2011/01/04_DARPA_Kicks_Off_Mind's_Eye_Program.aspx/ accessed 13.04.2011.

Department for Culture, Media and Sport (UK), Implementing the revised EU Electronic Communications Framework, April 2011. Online at www.culture.gov.uk/images/publications/FWR_implementation_Governmentresponse.pdf/ accessed 17.04.2011.

European Commission (2011). Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12.01.2011. Online at ec.europa.eu/information_society/policy/rfid/documents/info-2011-00068.pdf accessed 13th April 2011

European Commission Press Release (2011). Digital Agenda: new guidelines to address privacy concerns over use of smart tags. IP/11/418. 06.04.2011.

European Parliament (2010). Resolution of 15 December 2010 on the impact of advertising on consumer behaviour (2010/2052(INI)).

Fielding, N & Cobain, I (2011), Revealed: US spy operation that manipulates social media, The Guardian, 17th March 2011.

Franco-British Council (2010), How can France and the UK help citizens make better choices? 17th November 2010. Online at www.francobritishcouncil.org.uk/conferences.php?id=35/ accessed 10.04.2011

Gutwirth, S and De Hert, P (2008), Regulating Profiling in a Democratic Constitutional State, in Hildebrandt, M and Gutwirth, S (Ed), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer Science.

Hildebrandt, M (2008), Defining Profiling: A New Type of Knowledge?, in Hildebrandt, M and Gutwirth, S (Ed), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer Science.

Hill, S (2011), There's No Sense Stressing About the End of Privacy. E-Commerce Times, 15th April 2011. Online at www.ecommercetimes.com/story/72271.html?wlc=130293354/ accessed 16.04.2011.

Institute for Government (2010), MINDSCAPE: Influencing behaviour through public policy.

International Data Commissioners (2009), Madrid Resolution: International Standards on the Protection of Personal Data and Privacy, 6th November 2009. Online at www.hldataprotection.com/uploads/file/madridresolutionnov09.pdf/ accessed 10.04.2011

Internet Advertising Bureau (2011), Europe commits to self regulation. 14th April 2011. Online at www.iabuk.net/en/1/europecommitstoselfregulation140411.mxs/ accessed 16.04.2011.

Jarvis, J (2011), Revealed: US spy operation that manipulates social media,

Keats Citron, D (2010), Mainstreaming Privacy Torts, Cal. L. Rev, 98, 1805-1852.

Lessig, L (1999), Code and other laws of cyberspace, Basic Books.

Mckenna, A (2001), Playing Fair with Consumer Privacy in the global On-line Environment, Information & Communications Technology Law, 3, 339-54.

Melville-Brown, A (2008), Camera shy – the interaction between the camera and the law of privacy in the UK, International Review of Law Computers & Technology, Vol. 22, 3, 209-222.

Monmonier, M (2006), Geolocation and Locational Privacy: The "Inside" Story on Geospatial Tracking, in Strandburg, K and Stan Raicu, D (Eds), Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, Springer Science.

Narayanan, A & Shmatikov, V (2010), Privacy and Security: Myths and Fallacies of "Personally Identifiable Information". Communications of the ACM 53(6) June 2010.

O'Donnell, G (2010), Applying behavioural insight to health, Cabinet Office, 31 December 2010. Online at www.cabinetoffice.gov.uk/resource-library/applying-behavioural-insight-health/ Accessed 10.04.2011.

Office of Fair Trading (2010), Online Targeting of Advertising and Prices: A market study, OFT131, May 2010.

Ohm, P (2010), Broken Promises of Privacy: Responding to the Surprise Failure of Anonymization, 57 UCLA Law Review 1701-1777.

OUT-LAW News (2011), EU privacy law will extend to US social networks, vows Commissioner. 17th March 2011. Online at www.out-law.com/page-11824-theme=print/ accessed 17.04.2011.

Prime Minister's Strategy Unit (UK) (2004), Personal Responsibility and Changing Behaviour: the state of knowledge and its implications for public policy.

Prosser, W (1960), Privacy, Cal. L. Rev, 48, 383-423.

Reding, V (2011), Your data, your rights: Safeguarding your privacy in a connected Privacy Platform "The Review of the EU Data Protection Framework". 16th March 2011. Speech/11/183. Online at europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183 accessed 03.04.2011.

Ross, J, Retail technology and the evolving shopper. Online at www.shoppersciences.com/storage/TheEvolvingShopper_v4_SHS.pdf/ accessed 12.04.2011.

Schermer, B (2011), The limits of privacy in automated profiling and data mining, Computer Law & Security Review 27, 45-52.

Simitis, S (2010), Privacy – An Endless Debate? Cal. L. Rev, 98, 1989-2005.

Soltani, A, Canty, S, Mayo, Q, Thomas, L & Hoofnagle, C (2009), Flash Cookies and Privacy. 10th August 2009. Online at ssrn.com/abstract=1446862/ accessed 12th April 2011.

Tirtea, R, Castelluccia, C and Ikonomou, D (2011), Bittersweet cookies: Some security and privacy considerations. ENISA, February 2011. Online at www.enisa.europa.eu/act/it/library/pp/cookies/ accessed 10.04.2011.

Vaizey, E – UK Minister for Culture, Communications and Creative Industries (2011), CBI forum on e-privacy and the digital economy – 29th March 2011. Online at www.culture.gov.uk/news/ministers_speeches/7997.aspx/ accessed 09.04.2011.

Van der Hof, S and Prins, C (2008), Personalisation and its Influence on Identities, Behaviour and Social Values, in Hildebrandt, M and Gutwirth, S (Eds), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer Science.

Warren S., and Brandeis, L (1890), The Right to Privacy, Harv. L. Rev, 4, 193-220.

Zarsky, T (2006), Online privacy, Tailoring, and Persuasion, in Strandburg, K and Stan Raicu, D (Eds), Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, Springer Science.