4th International Conference on Information Law

Values and Freedoms in Modern Information Law and Ethics

20th and 21st May 2011 Thessaloniki/Greece

Digital Confidence - Is Europe's Information Society ready for a shift from state driven data protection to user driven data management?

Rechtsanwalt Dr. Marco Rau, Mag. iur. (Mainz/Paris XII), Maître en droit (Paris XII)

Corporate Affairs & Strategy

Telefónica Germany GmbH & Co. OHG, Munich/Germany

I. Introduction

Secrecy of telecommunications and user anonymity are classical distinguishing features of telephony and (mobile) internet usage. However, this freedom not to be supervised in the private use of internet and telecommunication services is in danger: technical development of tracking and data collection tools on the web as well as data warehouses challenge the basic concept of anonymity, in particular on the internet[1]. This is in particular true as customer data, mirroring clients behavorial patterns and needs for consumption have become highly valuable assets in the online world[2].

As telecommunication providers are shifting to become online companies[3], the provision of secure information/data services to customers is more in the public focus

[1] Nationaler IT-Gipfel Dresden 2010, Offen für die Zukunft – Offen in die Zukunft, p. 78 and p. 90 sqq.

[2] Some figures that may illustrate this development: in spring 2010 out of 82 million Germans 49 million older than 14 years used the Internet from time to time (69.4%), this is equivalent to an increase by 5,5 million user compared to 2009 [according to an online study conducted by German broadcasting channels ARD/ZDF, see *http://www.ard-zdf-onlinestudie.de*]

[3] See http://www.telefonica.com , Telefónica press release 5th of April 2011 entitled "Telefónica forecasts a future of growth shaped by innovative companies able to transform their businesses"

than ever. Probably next generation products of such telco-online companies will include a wide variety of personalized services – while always ensuring full control of such personal data by the customer. This said, implementation of EU Commission's Communication "A Digital Agenda for Europe"[4] becomes highly important.

New convergent (mobile) internet products include geolocation services and social networks of various kinds. In this regard European ICT industry companies must look beyond the short term legal requirements of data protection and unfair competition law[5].

Both, digital natives as well as digital immigrants[6] want control over their personal data, however digital natives[7] might agree in a different use of their personal data. Prerequisites for such more flexible use of personal data are *(i)* transparency and the possibility of informed consent, *(ii)* choice and privacy by design *(iii)* choice and right to be forgotten, as well as *(iv)* assurance of information security on highest levels. Implementation of digital confidence principles with new ICT industry products is necessary in order to overcome fragmental digital markets, cybercrime risk and low trust in networks in Europe. This will inevitably lead towards more user driven data management with regard to telecommunication and online services.

In this regard, self-determined use of information techniques and tools becomes highly important. This article analyses potential measures to successfully reach these goals.

[4] COM(2010) 245 final/2

[5] See for a focused overview on the multitude of European regulations on unfair competition practices in Europe: *Köhler*, in: Hefermehl/Köhler/Bornkamm, Gesetz gegen den unlauteren Wettbewerb, 27th edition, 2009, UWG (introduction) no. 3.41 sqq. (page 60 sqq.).

[6] Elder European Citizens may even require additional teaching with regard to the basic use of ICT and improve their overall technological abilities, see *Telefónica*, Corporate Responsibility Report 2008, page 38 sqq.

[7] Prensky, Marc, Digital Natives, Digital Immigrants, in: On the Horizon, Vol 9 No. 5, October (MCB University Press), page 3 sqq.

II. New Mobile Internet Products challenging data protection law

1. Substantial increase in smart phone use & location data based services

New mobile (online) products such as for instance mobile apps, helping to reduce roaming costs may require irregular but repeated access to user and location data. Thus, such new mobile products rely on personal data in order to provide the services demanded by the customer[8]. This is why, innovative location based mobile internet products[9] require the possibility for users to give their consent and expressly agree with multiple processing actions.[10] In this regard a possible near future scenario of digital propositions to customers includes information on traffic situations regarding the respective user's daily travel to work (e.g. including traffic information and/or restaurant recommendations).

a) Location based services

Several future mobile internet services will refer to and rely on customer location data. This data is in particular sensitive when it comes to profiling citizens' behavior[11]. Hence the use of such data in upcoming ICT industry products demands highest levels of control and security to generate the trust required for successful launch of such products. Upcoming legislation in the telecommunication sector in Germany already provides for a more flexible solution with regard to the provision of location based data under § 98 TKG-E ("German draft telecommunication law")[12]. If a user is running a self-triggered location service, a single informed consent by the user when downloading the app is considered to be sufficient to meet § 98 paragraph 1 TKG-

[8] http://www.telmap.com

[9] See as an example for geo-location data based navigation app products, http://www.telmap.com.

[10] See TKG-E 2011 [German Draft Telecommunications Law], reasoning as published by the German Federal Ministry of Economy on March 2nd, 2011.

[11] See Green German MP Malte Spitz movements overview, based on Deutsche Telekom Data mobile phone data combined with Twitter, Blogs and other Websites at http://www.zeit.de/datenschutz/malte-spitz-data-retention (English version entitled "tell-all telephone").

[12] See legal materials with regard to § 98 TKE-E ("German draft telecommunication law 2011"), page 144.

E criteria. This means that for locating the user's own device, i.e. the one with the MSISDN used for registration, a single approval of the respective client is sufficient when downloading the application. However, if such services should include a positioning/location finder service function provided to a third person[13], the user of such service must be informed via a SMS at each position finding. The draft law provides no right of objection to such SMS.

The importance of personal location data for future digital products is already visible to a greater public today. Therefore, the idea of classifying smartphones and other electronic devices according to the level of automatic production and background transmission to networks of personal location data[14] has been discussed in the European public. However, as most producers of smartphones, tablet computers and other relevant devices originate from Asia, US[15] or other destinations outside EU borders, EU Member State Governments should refrain from searching for national legislative solutions in this area of technical data protection. A recommendable solution appears to trigger a standardization process with a relevant international standardization body like ETSI[16] or ANSI[17] that obliges device producers to provide smartphones and tablet computers according to predefined high standards of privacy by technical design.

[13] http://www.foursquare.com

[14] See http://hackerne.ws/item?id=2469375 ("Hacker News" discussion/postings to "Apple is not recording your moves" (last visit 28th of April 2011); See German IT-Weblog on further information with regard to a "Datenausweis": http://www.it-weblog.de/tag/datenausweis/ (last visit 28th of April 2011); "Golem" German IT-Webportal specialized in ICT news http://www.golem.de/1007/76847.html "App-Genom-Projekt" - "Android App sammelt persönliche Daten und gibt sie weiter" (dated 29 July 2010, last visit: 28th of April 2011)

[15] See for further information on current legal disputes between Apple and its competitors: *Postinett*, in: Handelsblatt 20th of April 2011, page 18 sqq. "Apple gegen den Rest der Branche".

[16] http://www.etsi.org/WebSite/homepage.aspx

[17] http://www.ansi.org

b) New mobile online services and consumer protection

Increased use of smart phones[18] and location based services, like real-time navigation services, might lead to conflicts between (telecommunication law) data protection requirements, civil law consumer protection regulations and general civil law principles. A recent ruling of the District Court of Bonn/Germany[19] revealed that the aforementioned scenario is a relevant consumer protection issue. In this case a customer sued a telco provider as her bills amounted up to EUR 5000 due to intense smartphone use within a 5 months period. While the customer's mobile internet tariff still was calculated on a minute based billing the customer's rooter was constantly online.

The Court ruled that the telco provider had violated information obligations deriving from the valid telco services contractual relationship with the customer. Hence, it would have been the telco provider's obligation to react due to unusual user behavior within a reasonable (few days) delay. According to the Court's reasoning, appropriate provider reactions would have included internet access blocking – while simple waiting for next invoices to be sent to customer was considered inappropriate business behavior. However, the Court did not analyse in further detail problems of telecommunications law.

Anyway, it is important to state that the provider may – upon stating an unusual usage behavior by the customer – inform the customer thereof and signalize discrepencies compared with invoiced sums before. However, an in-depth review of traffic data by the telco provider did not appear to be permissible to the Court as according to applicable data protection regulations this shall only be allowed to design or adopt telecommunication services on condition that a respective consent has been provided by the customer in beforehand[20]. Thus, if such a specific consent

[18] The Wall Street Journal, April 20th 2011 "As Nokia shifts, it is back to basics" article by Christopher Lawton arguing that the ratio of smartphones to simple feature based phones is rapidly changing. In 2010, smartphones accounted for 22 % of global handset shipments, versus 15 % in 2009. That percentage is expected to jump to 45 % by 2015.

[19] District Court of Bonn, file number: 7 O 470/09

[20] See supra § 96 paragraph 1 and 3 German Telecommunications Code; Legal opinion of the German Federal Commissioner for data protection and information security (assessment of Bonn District Court Decision 7 O 470/09).

to track the customer's user behavior with mobile data services has not been asked for and provided in beforehand, the telco provider has to ask for specific permission as stipulated by law[21]. Altogether the case showed, that data protection laws might under certain circumstances conflict with maximum consumer rights and interests.

2. Social Networks

Modern online-oriented companies focus on social network communication with their clients as well as development of products orientated on social network discussions. Social media may be described through 3 layers *(i)* a socio-economic layer *(ii)* a technological layer as well as *(iii)* an individual layer[22]. Opposed to earlier internet techniques, the world-wide experienced phenomenon of social media focuses on the individual. Each and every single social media user might at the same time produce contents, play an active or a passive role, be a consumer or a producer of content[23]. Thus, social media constitute a massive challenge for classical European data protection law principles[24] such as the paradigm that personal data may not be processed as long as there is no special permission (by explicit consent or law) as well as that personal data may only be processed for a certain predefined purpose.

Social media users can be active or passive members of a community, changing between a consumer and a producer role. Hereby a large number of users can be reached. This said, Social Media make it hard to define precise frontiers between users and companies, content industry and consumer as well as employees and customers. Social media such a Twitter[25] form an integral part of today's real-time parallel media usage – as for instance used by Pierce Morgan, talk-show host of

[21] See for further detail on this case: legal opinion provided by the Federal German Officer for data protection and information security, in: "Tätigkeitsbericht für die Jahre 2009 und 2010" - Der Bundesbeauftragte für Datenschutz und Informationssicherheit, page 80 sqq. – see: (http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile)

[22] Michelis, in: Social Media Handbuch – Theorien, Methoden, Modelle, p. 301

[23] This is in particular true when it comes to rating websites such as http://www.rottenneighbor.com (originally an US American website for neighborhood ratings blocked for German IP number holders) or "spickmich.de" (a German teacher rating website).

[24] Scheider, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip, Modernisierung des BDSG mit einem neuen Ansatz – und mit 12 Thesen zu einem Stufenmodell, Anwaltsblatt 2011, page 233.

[25] Http://www.twitter.com

CNN's nightly talk – to reach more than 500,000 followers when breaking news make his CNN television format the attractive choice of the soirée[26].

Another proof of the fact that interaction between individual and technical layers of the internet has lead to a multiplicity of trends are authentic forms of communication, symmetric relationships between users and (content) providers. But this assessment unevitably arouses the legal question to what extend social media use may imply "willful writing away parts of privacy"[27].

Therefore, as to the future use of Social Networks focused on publishing functions like "rating platforms" the protection and effective control of the user's digital identity as such appears to be core rather than regulating the sourcing and processing of the respective personal data.

Besides this rather user driven form of publishing of personal private data on social media another relevant aspect as to processing of personal data is the evaluation of customer volunteered personal data for marketing and product positioning purposes. Due to different approaches as to the all over extent of such use within the data industry worldwide[28], in particular this latter aspect of data usage is less known to the public. From a data protection perspective today's upfront corporate communication departments use social media channels to interact with customers at eye-to-eye level. Specific product defaults are being solved in chat spaces by way of direct interaction between user and IT companies' service employees[29].

Most importantly when it comes to social media usage, marketing departments try to analyze social media to unveil, model and exploit real social networks. Of course it is advantageous to understand these dynamics to provide customized solutions and

[26] Financial Times Weekend, April 16/April 17 2011, Life & Arts, page 3, interview of FT journalist Andrew Edgecliff-Johnson with Piers Morgan entitled "I don't have pomposity".

[27] This is in particular true when it comes to Social Media that feature aspects of "online journalism" and/or "reporting". In those cases of content production for a broader public - literature content / editorial content - the "media privilege" may suspend application of data protection law principles (e.g. realtime online journalism cannot provide prior valid consent to each and every processing of personal data); see BGH 23th of June 2009, file number VI ZR 196/08 – spickmich.de

[28] Further information on data mining practices can be found under *Scholz*, in: Roßnagel, Handbuch Datenschutz, Chapter 9.2 sqq. (page 1837 sqq.).

[29] See Telefónica Germany chat and client space at http://www.o2.de

products, in particular to digital natives. As in the offline world, marketing departments appreciate information that provides insights as to the customers' social context including contacts, communities and his/her social role. Having roughly understood modeling of viral effects and prediction of spreading paths within the targeted groups using social media for daily communication, meeting consumer needs is easier. This includes knowledge on the viral spreading process within social groups after a costly advertising campaign or to better understand churn rates. In-depth knowledge and of social networks therefore is very attractive to companies as it enables (i) churn rate reduction, (ii) identification of positive influences for advertising campaigns as well as (iii) better targeting of products and services to customers.

However, these commercial motivated goals and actions might easily collide with data protection regulations if no transparent communication of provided opt-ins by the customer is accessible [e.g. in a large, self-explanatory tableau graphic]. If the customer has easy online access and knowledge of all opt-ins ever provided to a provider a high level of transparent personal data processing is ensured as requested by EU Commission[30].

Given this background of sensitive personal data to be processed by social networks, Germany's printing press[31] and data protection doctrine has focused on Facebook's privacy practices for a longer period[32]. Even though Facebook is still less used in Germany than in the UK or US[33], this international social network leads to a wide range of legal questions as from German and European Data Protection Law perspective: data collection from Facebook members has impact on non-members through Facebook's address book search function. This way Facebook collects mail addresses from subscribers and non-subscribers of the network. In case a user wants to prevent Facebook from sharing non-member addresses from using non-

[30] COM (2010) 609 final, page 9

[31] See with further details a instructive article in Germany's Frankfurter Allgemeine Zeitung ("FAZ") dated 17 October 2010 "Spionieren mit Facebook" by Stefan Tomik at: http://www.faz.net/s/Rub594835B672714A1DB1A121534F010EE1/Doc~E5205C93A4508472CB610D9565E72C5BD~ATpl~Ecommon~Scontent.html

[32] Erd, in: Tagungsband DSRI Herbsttagung 2010 Digitale Evolution, Datenschutz in Sozialen Netzwerken am Beispiel Facebook, page 321

[33] see http://en.wikipedia.org/wiki/Facebook

member addresses with the user's environment, such user needs to actively delete them. As communication via social media becomes a substantial part of daily internet usage, various national legislative initiatives throughout Europe try to tackle the problem of data protection via security pre-settings and other regulations.

c) Social media and current legislative initiatives

Adopting current legislation throughout Europe to social media privacy challenges has triggered legislative proposals and legal debate in various fields in France[34], Germany and the rest of Europe.

From a German perspective it appears that a more structured and focused approach should be taken towards different forms of internet technology and usage. So far legislative proposals rather featured a case by case approach than trying to execute a real paradigm change.

In Germany for instance the Land Hessen has recently introduced a legislative proposal as to § 13 TMG ("Telemediengesetz / Telemedia Act") that should be amended by a newly introduced § 13 a TMG[35], including a responsibility for the provider of a social network to always use maximum restrictive data protection pre-settings when a user subscribes to a social network. This maximum restrictive presetting shall avoid any external search engine to find the subscriber to a social network without his explicit, informed consent. Moreover, a detailed and easy to understand consumer information shall be provided at the time of subscription, informing about the personal settings of the customer and potential privacy risks. It remains to be seen how this legislative proposal relates to other initiatives such as another planned German federal legislation „Rote Linie Gesetz" ("red line law"). This new legislation as a reaction to Germany's Bundesgerichtshof decision "spickmich.de" would be intended to provide enhanced protection against

[34] "Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique", adopted upon 1st lecture by the French Sénat 23 March 2010 (TA n° 81). This draft law has been transferred to "La Commission des lois constitutionnelles , de la legislation et de l'administration générale de la République for further discussion and review by Assemblée Nationale. The draft law inter alia calls for a new educational approach leading towards a "homo numericus".

[35] Proposition of the State of Hessen to the Federal Council of Germany ("Bundesrat") dated 19 March 2011 regarding an amendment to the German Telemedia Act (§ 13 a TMG) on duties of telemedia service providers including user generated content.

unauthorized publishing of personal data on the internet. In its leading case "spickmich.de" Germany's Bundesgerichtshof had found in 2009 that personal data sourcing, saving as well as transmission to a 3rd Party might be acceptable under certain circumstances even though no prior consent had been given by a teacher rated by a teacher rating website for pupils[36]. The Court argued that besides classical personal data such as date and place of birth, personal views and statements that relate to a certain person constitute personal data. For sourcing, saving and transmission of such personal data as a rule the entire set of the German Federal Data Protection Code ("BDSG") regulations apply. Therefore, sourcing and storage of personal data for transmission purposes to a 3rd party is permitted according to section 29 BDSG if there is no opposing elementary interest of the individual in question. In this specific case the German Court of Justice ("BGH") found that the acclaimed opposing interest (i.e. the right to informational self-determination was overweight by the colliding right of freedom of speech as exercised on the rating platform).

3. Turning young people into active digital citizens

In the near future young people might be especially attracted by new LTE technology based products[37]. Today's children in Western countries are digital natives[38] and dispose of many qualities in modern technology usage which their parents did never acquire. Therefore, (i) ensure childrens' safety when using the internet, as well as (ii) enabling them to consume and use multimedia products reasonably[39] is key for any long-term privacy orientated EU Commission and industry driven internet strategy[40]. As the internet itself, the gaming industry is very international as can be easily seen on the example of mobile products facing different legislative requirements than other fields throughout Europe[41]. However, especially offers to

[36] BGH, decision dated 23 June 2009 file no. VI ZR 196/08 = MMR 2009, 608 sqq.

[37] KJM informiert 2010/2011, p. 9

[38] Prensky, Marc, Digital Natives, Digital Immigrants, in: On the Horizon, Vol 9 No. 5, October (MCB University Press), page 3 sqq.

[39] See e.g. Telefónica o2 UK information booklet "Who wnts 2 no?"; Fechner, Medienrecht, page 128

[40] EU COM (2010) 609 final, page 9

[41] Multimedia und Recht 2009, EMR – die medienrechtliche Monatsschau, page XIV „Österrereich: Neuerrungen im Jugendschutzrecht – Kennzeichnungspflicht für Computerspiele"

young people must be considered both from a data protection law as well as a youth protection law perspective[42].

In this regard it is important to understand that EU Member States legislation on youth protection as well as data protection legislation still differ throughout Europe[43]. For example mobile game products that include certain violent acts or pornographic posing may be permissible under Netherlands Law but might be prohibited under German youth protection law[44]. After all youth protection laws and youth protection surveillance body organizations still show a variety of approaches throughout the European Union[45]. According to current legislation minors are not able to provide valid consent into data processing operations but they nevertheless form an integral part of the net generation. Being strong users of mobile gaming and social media offers an enhanced European legal framework, both for legal requirements as to offers to minors on the as well as with regard to a harmonized organization of surveillance bodies[46] appears to be advisable.

III. New perspectives

1. Transparency and the EU Commission's Communication "A comprehensive approach on data protection in the EU"[47]

An early computer ethics topic to arouse public interest was privacy[48]. Therefore US philosophers and lawyers were intensely confronted with computer system related

[42] Multimedia und Recht 2009, EMR – die medienrechtliche Monatsschau, page XIII „EU: Mehr Sicherheit für Kinder im Internet"

[43] ECJ decision C-244/06 dated 14 February 2008 (marginal number 14 sqq.), „Dynamic Medien"

[44] Lischka, Konrad, in: Spiegel Online: Jugendschutz – Bundesgerichtshof prüft Online Altersnachweis (18 October 2007) at http://www.spiegel.de/netzwelt/web/0,1518,512186,00.html

[45] ECJ decision C-244/06 dated 14 February 2008 (marginal number 14 sqq.), „Dynamic Medien"

[46] Frey, Dieter/ Rudolph, Matthias, Der Jugendmedienschutz-Staatsvertrag im Lichte des Gemeinschaftsrechts, ZUM 2008, page 572

[47] COM(2010) 609 final

[48] Stanford Encyclopedia of Philosophy, Computer and Information Ethics, see: http://plato.stanford.edu/entries/ethics-computer/

data protection issues already in the mid-1960s when the American government intended to create a large data base of information of its citizens. Ever since the variety of privacy related issues generated by computer technology has led philosophers to rethink as well as to re-examine the concept of privacy itself.

Transparency and free flow of information are vital for modern, user orientated and user controlled data processing – they are prerequesite for the free unimpeded use of the internet resource as such[49]. This term as used in a social and information system design context means in particular openness, communication and accountability[50]. Thus, transparency as far as digital openness is concerned, inevitably includes aspects of intelligent information management and modeling of human user interfaces and portals. To ensure transparent ways of customer driven data processing the classical chain of knowledge gaining must be observed: (i) data [symbols] – (ii) information [data that are processed to be useful] – (iii) knowledge [application of data and information] - (iv) understanding [appreciation of "why"] – (v) wisdom [evaluated understanding][51]. Transparent processing of (personal) data therefore in a first step includes implementation of architectures that offer easy to handle access to all data stored with relation to the customer. But it is even more important in a second step to provide understandable information that enables customers to do customer driven data management, i.e. customers should be

[49] This is especially true as in a recent case Google was fined by France's privacy protection body CNIL (Conseil National de l'informatique et des Libertés) over the personal data it mistakenly gathered when setting up its digital product "Google Street View" throughout France. The internationally perceived EUR 100,000 penalty is the largest handed out by CNIL since its foundation in 1978. The fine is punishment for Google mistakenly scooping up personal data from Wifi networks while taking pictures for Street View from 2007 onwards. Google has apologized in public for this grave mistake and said it would delete the data concerned. The data from open Wifi networks was gathered while so called "Google Street View Cars" roamed Europe from 2007 – 2010, taking photographs. Upon levying the fine, CNIL criticized Google for its conduct during its investigation. "They were not always willing to co-operate with us, they didn't give us all the information we asked for, like the source code of all devices in the Google cars. […] They were not always […] transparent." declared CNIL's director in an official statement with regard to the administrative fine awarded (see for further information as to these proceedings: http://www.cnil.fr).

[50] See for further background information on the wide notion of „transparency": http://www.wikipedia.org „transparency (behavior)"

[51] The knowledge/wisdom creation process taken from: Bellinger, Gene/ Castro, Durval/ Mills, Anthony, "Data, Information, Knowledge and Wisdom"(2004), http://www.systems-thinking.org/dikw/dikw.htm

enabled to execute a risk assessment as to each and every possible data processing action[52].

Drawing up one or a set of imperative EU standard forms (e.g. “privacy information notices” as well as “data processing risk level standards”) to be used by data controllers could be helpful to achieve high and uniform European standards for the ICT industry. Finally it is important for individuals to be informed when their data is accidently or unlawful destroyed/lost – to enhance customers’ confidence in such data breach notification processes it is advisable to agree upon an uniform European standard procedure for such incidents that should be presented to the European public.

2. Outlook: Digital Confidence & paradigm change

Today internet usage differs substantially from those times the EC Data Protection Directive 95/46 was established. Local networks and data processing units were substituted by highly integrated international networks[53].

a) Transparency and a new model of informed consent

As telecommunication providers are shifting to online companies it is important to make customers understand that many next generation digital business models such as location data based social network services use personal data.

It is core for online and telco companies to reposition from private communication service providers and make customers understand that new digital service models are based on customer data. Since classical “state law driven” data protection is loosing grounds with regard to next generation digital propositions provided on a global scale, only such products that go beyond state driven protection by enhanced control mechanisms have a raison d’être. Thus, classical “box ticking” as required by today’s EU Member State unfair competition and data protection laws in transposition

[52] Schneider, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip. Moderniiserung des BDSG mit einem neuen Ansatz – und mit 12 Thesen zu einem Stufenmodel, page 239 [arguing for a risk assesment system that at least indicates levels of risk exposure „green“, “yellow“, „red“].

[53] Schneider, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip. Modernisierung des BDSG mit einem neuen Ansatz – und mit 12 Thesen zu einem Stufenmodel, page 233

of EU legislation[54], is no longer appropriate to cover upcoming technologies and IT industry propositions.

In order to comply with the basic right of self-determination, as protected by the EU Charter of Fundamental Rights and EU Member State Constitutions[55], a new mechanism of user driven sourcing of data has to be implemented[56].

Such user driven sourcing of personal data should be done in a new kind of user driven dialogue between customer and company. This process could be executed via a random gaming process. In particular digital natives like to parallel process and multi-task. They prefer gaming to serious filling out of a questionnaire[57]. Hence the kind of dialogue led self-experience to source data appears to be one future scenario how personal data and core sphere data could be raised.

Results should be sorted according to different categories like “personal interests”, “financials”, etc. Having full access to his personal data, each user should be enabled to decide in a second step, if he would like to mix certain categories (like green data pot with a yellow data pot) of data resulting in new assessments. Thereafter, in a third step the customer could decide if this data might be used for a digital offer.

Finally, the aforementioned user controlled personal data generation should be executed by only a few state licensed providers “digital identity hosting companies” underlying highest data security regulations. Altogether a multidimensional approach, including (i) a new model of informed consent, (ii) transparent and reasonable pricing for digital products, (iii) simple to use services as well as (iv) technology and expert guidance for minors must be provided to ensure transparency and obtain informed consent from customers with regard to new digital products.

b) Choice & privacy by design

A new approach must include a substantial design of digital products according to privacy by design principles. This includes a several layer system of personal data

[54] E.g. Directive 2005/29/EC, Directive 2006/114/EC, Directive 2000/31/EC, Directive 2002/58/EC etc.

[55] See inter alia Art. 2 paragraph 1 Grundgesetz (“German Constitution”)

[56] COM (2010) 609 final, page 5

[57] Prensky, Marc, Digital Natives, Digital Immigrants, in: On the Horizon, Vol 9 No. 5, October (MCB University Press), page 2.

protection, providing different protection levels until at the highest level – core intimacy information or "informational privacy sphere"[58] – is reached.

c) Exit scenarios: choice, right to be forgotten, data portability

In order to fulfill data control principles with regard to digital identities, deletion of personal data must be full an final (e.g. in case of a change in providers). As Austria's High Court stipulated in a recent ruling[59], that a "blocking" of data as well as a "logical deletion" (i.e. personal data is no longer accessible within a closed IT-System) does not satisfy such deletion criteria. Moreover a user of next generation digital services should be enabled to take all such data away after expiry of a respective contractual period – for instance in easy customer to handle standard file formats[60]. This way a maximum of data portability would be ensured to the benefit of the customers.

d) Highest IT-Security Levels

Administration of digital identities will require highest IT-Security standards[61] from digital identity hosters. This includes ensuring (i) accessibility and confidentiality, (ii) integrity, to ensure full content integrity (iii) authenticity to ensure that each and every data set is bound to a sole customer identity, (iv) control of each and every data processing.

e) Conclusion

European Information Society requires easy to handle, secure ways of exchanging data and processing such data in order to benefit from new (mobile) internet technologies on the rise. To meet technical requirements and at the same time providing highest level of data protection a paradigm change in European data protection law is required.

---

[58] Schneider, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip, Anwaltsblatt 4/2011, page 238 – see rulings of the German Constitutional Court, BVerfG 15th of December 1983 „Recht auf informationelle Selbstbestimmung" and BVerfG 27th of February 2008 = Computer & Recht 2008, page 306 „IT-Grundrecht"

[59] Austrian High Court, ÖGH 15th of April 2010, file number: 6 Ob 41/10p (OLG Wien, LG Wien); Multimedia und Recht („MMR") 2011, page 204 sqq.

[60] In transposition of EU Commissions recommendations as stipulated in COM (2010) 609 final, page 8

[61] See in further detail on modern standards for IT Security relevant user driven administration of digital identities: Rossnagel/Federrath/Pfitzmann, Handbuch Datenschutz, Section 2.2. no.5 sqq.

Responsibility for data protection in the non-public sector should be shifted from state driven and state enforced data protection mechanisms to more user driven[62], a more company – customer oriented relationship to ensure privacy. Given today's tracking scenarios in public transportation systems, CCTV installations and social network profiles of various kinds, the notion "privacy" must be redefined.

This will include an intense debate on the relation between freedom of speech, free flow of information as well as "core spheres personal data". In this regard, several layers of a digital identity should be defined – whereas the inner core would be protected against any kind of processing without explicit consent by the owner of the digital identity, whereas other strings of personal data could be processed according to weighting of interests process according to criteria predefined by law[63]. On the one hand the customer rights to information become highly important[64] in this new user – online company relationship (e.g. including at times different stakeholders worldwide when providing an app service). On the other hand online companies become hosters of digital identities, offering a better quality of life through a variety of digital products going beyond simple telco services.

This new approach outlined above means a paradigm change in European data protection law from state driven to more user driven data protection. This implies a substantial challenge in the way data protection should be secured in the future. European Information Society should accept the challenge of a paradigm change as to the protection of its citizens' and their digital identities.

[62] Rau/Behrens, Kommunikation und Recht 2009, page 771

[63] Schneider, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip, Anwaltsblatt 4/2011, page 238.

[64] See the "Holy Grail" of Germany's data protection law structure, § 34 BDSG ("access rights"), Meents, in: Taeger/Gabel (Editors), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, § 34 BDSG no. 3

Literature

1. Manuals / Commentaries

Arnold Picot/ Said Zahedani/ Albrecht Ziemer (editors), Spielend die Zukunft gewinnen – Wachstumsmarkt elektronische Spiele, Springerverlag Heidelberg 2008

Daniel Michelis/Thomas Schildhauer [Hrsg.], Social Media Handbuch – Theorien, Methoden, Modelle, NOMOS 2010

Fechner, Frank, Medienrecht, 4th edition, Mohr Siebeck Tübingen 2003

Erd, Rainer, in: Tagungsband Herbstakademie 2010, Digitale Evolution – Herausforderungen für das Informations- und Medienrecht, OLWIR Editors 2010

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., Jahresbericht 2010, FSM Berlin 2010

Nationaler IT-Gipfel Dresden 2010 – Münchner Kreis/EICT GmbH/Deutsche Telekom AG/TNS Infratest GmbH/Siemens AG/Vodafone D2 GmbH/SAP AG/Telefónica o2 Germany GmbH & Co. OHG/Zweites Deutsches Fernsehen, Rasch Verlag November 2010

Taeger, Jürgen (Editor), Bundesdatenschutzgesetz, Verlag Recht und Wirtschaft, Frankfurt am Main 2010

2. Articles / legal opinions

Financial Times, April 16/April 17 2011, Life & Arts, page 3, interview of FT journalist Andrew Edgecliff-Johnson with Piers Morgan entitled “I don’t have pomposity”.

Legal opinion of the German Federal Commissioner for data protection (legal assessment of the Bonn District Court Decision 7 O 470/09) in: “BfDI - Jahresbericht 2009/2010”, see: (http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile)

Frey, Dieter / Rudolph, Matthias, Der Jugendmedienschutz-Staatsvertrag im Lichte des Gemeinschaftsrechts, ZUM 2008, 564 - 572

Prensky, Marc, Digital Natives, Digital Immigrants, On the Horizon (MCB University Press, Vol. 9 No. 5, October 2001), see:

http://www.marcprensky.com/writing/prensky%20-%20digital%20natives,%20digital%20immigrants%20-%20part1.pdf (last download 2011/04/18).

Rau, Marco/Behrens, Martin, Catch me if you can…Die mittelbare Haftung der Betreiber von Anonymisierungsdiensten …, Kommunikation und Recht 2009, pages 576 - 586

Schneider, Jochen, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip – Modernisierung des BDSG mit einem neuen Ansatz – und mit 12 Thesen zu einem Stufenmodell, Anwaltsblatt 4/2011, pages 233 - 239

Stanford Encyclopedia of Philosophy, Computer and Information Ethics, see: http://plato.stanford.edu/entries/ethics-computer/

Tomik, Stefan, in: Frankfurter Allgemeine Zeitung (“FAZ”), dated 17 October 2010 “Spionieren mit Facebook”

3. Legislative materials / Compendia

German Draft Law for a telecommunication law („Kabinettsentwurf Telekommunikationsgesetz 2011“), 2nd of March 2011

European Commission „A digital Agenda for Europe“ [COM(2010) 245 final/2]

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “A comprehensive approach on personal data protection in the European Union”, COM (2010) 609 final, Brussels 4th of November 2010

GSMA Europe response to the European Commission consultation on “A comprehensive approach to personal data protection in the EU”, 15th of January 2011

Kommission für Jugendmedienschutz der Landesmedienanstalten (Hrsg.): Positionen zum Jugendmedienschutz in Deutschland. Eine Textsammlung. KJM-Schriftenreihe, Band 1, Vistas Medienverlag Berlin 2009

Kommission für Jugendmedienschutz der Landesmedienanstalten (Hrsg.): Umstritten und umworben: Computerspiele - eine Herausforderung für die Gesellschaft. KJM-Schriftenreihe, Band 2, Vistas Medienverlag Berlin 2010

Telefónica S.A., Corporate Responsibility Report 2008