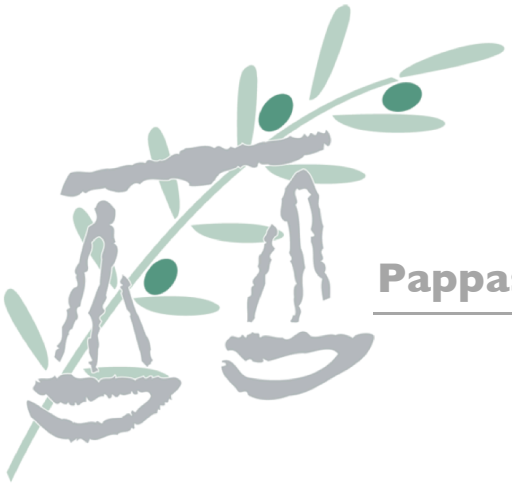
EU-nomia no. 1
European Law & Policy, June 2012



Pappas & Associates

Attorneys at law

Inside this issue:

Privacy and Data Protection

PAPPAS & ASSOCIATES
Rue Stévin 49/51, B-1000 Brussels, Belgium * Tel: +32(2)23 15 704-5, Fax: +32(2)70 64 829
www.pappaslaw.eu * Email: info@pappaslaw.eu

Pappas & Associates
Attorneys at law

At a turning point: old versus new society?

Spyros A. Pappas

One of the deepest philosophical foundations of the EU is the absolute value of the individual. It is on this value that democracy is based and the EU in its turn on the latter. Although of absolute character it is not unlimited. It reaches its borders at the line of respect of the other.

One aspect of the value of the individual is privacy. Directive 95/46/EC has so far generally been hailed as being a success and a pioneer in data protection all over the world in particular thanks to its technology-neutral character and the underlying, flexible principles[1]. It encompasses two general objectives of the EU: the protection of fundamental rights and freedoms of the individuals, in particular the right of protection of personal data (Art. 8 of the Charter of Fundamental Rights of the European Union, now legally binding), and the free flow of the said data in the internal market (attainment of a common market). The Directive though has come to face challenges of the EU legal system and of our time. Social networking sites, cloud computing, e-government, e-commerce, globalization are some of the factors that have transformed the current technological landscape beyond recognition and "imposed" their own reality.

By way of example, suffice to look at the case study of Google leading in the field of search engines:

➢ In 2007, Art. 29 Working Party (the EU independent advisory body set up by the 95/46/EC Directive) urged Google to store server logs (users' web history data, which is identifiable "personal data" in the meaning of the Directive) generated by Google users for a reduced period of time, as two years was too long[2]. Google failed to specify why it needed to keep this data for so long, as required by Art. 6(1)(e) of the Directive and also why the "Google cookie" had a lifetime of thirty years manifestly going far beyond what is "strictly necessary" for Art. 5(3) Directive 2002/58/EC.

---

[1] Notice - Individuals must be informed that their data is being collected and about how it will be used.
Choice - Individuals must have the ability to opt out of the collection and forward transfer of the data to third
Choice - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
Onward Transfer - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
Security - Reasonable efforts must be made to prevent loss of collected information.
Data Integrity - Data must be relevant and reliable for the purpose it was collected for.
Access - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
Enforcement - There must be effective means of enforcing these rules.

[2] It should be noted that two years is the period of time Google decided to adopt after a change of policy to reduce this amount of time; before this incident it stored personal data indefinitely!

Pappas & Associates, Attorneys at law, 49-51, Rue Stévin, B-1000 Brussels, Belgium
www.pappaslaw.eu, email: info@pappaslaw.eu, tel.: 32-2-23 15 704-5

- From 2007 to 2010, Google, via its Street View service, had access and was amassing information available on public Wi-Fi networks in most EU countries (and all over the world too, e.g. New Zealand), including all Internet activity of users, the content of their e-mails and potentially even hard drive content, without any notice or consent! This unprecedented breach of security and privacy came to light only after the Hamburg Data Protection Authority insisted on reviewing data accessed by Google Street View. Google has not accepted responsibility or explained why this happened.
- In 2009, it was found out that Google Docs Cloud Computing Service disclosed user-generated documents to users of the service without permission to view them.
- In 2010, Google's social networking site Buzz was launched, immediately contributing to the company's violations. Buzz, now inoperative, had a huge privacy flaw: its default setting allowed public viewing of the people the user mailed and chatted with the most –through Gmail- and it outraged users who fell its victims. Google finally settled claims with the Federal Trade Commission ("FTC") in the USA, accepting that it "used deceptive practices and violated its own privacy policies".
- In 2011, "Safarigate" or "Cookiegate"[3] was revealed, which truly appalled everyone watching. Apparently, Google had been circumventing Safari default privacy settings to serve personalized advertisements to users by spying on their research habits. Although the practice is hardly unusual in this business, the intentional circumventing is not only in contradiction to Google's own instructions to users on how to avoid tracking, but also evinces how unilaterally Google can act and manipulate users' identity elements, with virtually no consequence whatsoever for its actions.
- Finally, Art. 29 Working Party has warned Google to pause implementation of its new Privacy policy (uniting all its services' policies into one) so that the new privacy terms are checked. However, went on with its plans and implemented the new policy on 1st March 2012, as originally envisaged. The most important issue in this new policy will have to be cross-sharing, i.e. user-generated data collected across all of Google's numerous services. By implementing this new policy, Google also breaches the FTC agreement mentioned above, which provides that Google should allow users to opt in, in case its privacy policy changes.

The disregard of fundamental rights is obvious. Fragmented and outdated legislation offered an attractive vacuum to pioneering companies. Moreover, it became obvious that absolute values cannot but be of relative protection in a world driven by new market and societal features. As the EU Justice Commissioner recently put it: "Let us build a new gold standard of data protection based on clear and strong laws allowing our businesses and citizens to fully benefit from the digital economy."

In this context next to the objective of a single set of rules on data protection, valid across the EU, new concepts are on the agenda such as the right of informational self-determination. It contains:

-the right of easy access to one's own data and the right of data portability, i.e. easier transfer of personal data from one service provider to another;

[3] Term used by Greg Sterling from Search Engine Land.

-the principle of prior and explicit (not just assumed) consent for data to be processed;

- the 'right to be forgotten' will allow people when they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data to be deleted;

-the right to limited data retention.

The challenge remains enormous. It looks like the struggle between an outgoing world based on ideas in the center of which lies the Man versus an incoming world based on market and technology. No doubt the balance is not easy, yet of paramount importance for the quality of life. Besides, while legal certainty is at present required to create confidence, on the other hand flexibility, or adaptability is indispensable. In this regard, it is relevant to take into account the comparison between the ratio 1% of all telecommunicated information in 1993 to more than 97% in 2012 and a decision making that was reasonably quick and has become unreasonably slow. In between, people and data mobility will be increasing, as well as the occurrence of more and more commercial and financial transactions via the Internet resulting in the need for more cooperation throughout the EU on criminal matters (identity of criminals, child pornography, terrorism matters), all made possible through the evolution of technology. Will users manage to adapt themselves to new technological achievements? Will new legislation when adopted always be up to date? How will it be feasible to couple certainty with flexibility, both required? Questions that have no obvious answers once the basics are put into review.

Pappas & Associates
Attorneys at law

The Right to Informational Self-Determination: A Privacy Concept fit for the Future?

Stephan Dreyer
Senior Researcher at the Hans Bredow Institute for Media Research

Introduction

The "Right to Informational self-determination" has been an important approach in the field of data protection and surveillance since the 70ies. Since a well-known decision of the German Constitutional Court in 1983, it has been recognized as a specific extension of the basic right to personality, shaping the layout of data protection laws. Back then, it has been elucidated to react to new forms of risks by means of electronic information processing. The following article describes the legal and sociological theories behind the right to informational self-determination, its current challenges and the possibilities a concept of informational self-determination as such offers for today's information and communication regulation and practice.

Informational self-determination: Protection of freedom and democracy, not property in data

It already comes with the term *self*-determination. To determine, and not to be determined, is the objective of a right that aims at letting the individual's authority "to decide himself when and within what limits information about his private life should be communicated to others". And this is the premise of the right to informational self-determination the German Constitutional Court generally introduced in its famous public census decision (BVerfGE 65, pp. 1). This constitutionally backed right was not new, as some state, it was more like a cogent deduction of the existing judicature. It was the court's reaction to new risks for personal and/or personality rights that are accompanied with modern developments: The purpose of the right's birth was to put existing basic rights back on the map again in view of new threats in every day's life due to new technologies and procedures (Kunig 1993: 569).

And how life-altering these new technologies for data procession have been in 1983! From paper-based card indexes to electronic files and databases – storable, accessible and combinable virtually without limit, leading to a situation where people might not know who knew what about them in what contexts. Nowadays, we live in an age that is strikingly reminiscent to this deliberation, almost 30 years later.

The court based its decisions on two pieces of reasoning. Firstly, informational self-determination must exist to ensure individuals can develop their personality freely and without undue external interference. Living out these "autonomic capabilities" (Rouvroy and Poullet 2009: 46) – or shorter: enjoying this freedom – is what a right to informational self-determination has to aim at. The

approach builds upon concepts from system theory: According to *Luhmann,* the function of a concept of privacy aims at protecting the consistency of the personality (Luhmann 1995). This consistency relies on the separation of societal sub-systems. Only as long as these (personal) sub-systems are basically shielded from each other and no information from one system diffuses into another system (e.g. from medical treatment to work environment) self-determined development of the individual can be upheld (cf. Hornung and Schnabel 2009: 85). The court refers to (broader) constitutional guarantees, especially the general right to general personal liberty (Art. 2 sec (1) of the German Constitution), and, combined with the guarantee of human dignity (Art. 1 sec (1)), the concept of a general right of personality, giving each citizen the possibility to freely develop his or her own personality autonomously. This is the place where the court saw the potential of new risks of technological developments: If a person cannot predict with sufficient certainty what information about him is known to his counterpart or social milieu, the individual might see himself pressured to act "low-profile". In case a person is uncertain whether deviant behaviour is being monitored, noted and stored as permanent information, he will try not to attract attention by such activities. Such consequence, however, is exactly what a general right to autonomously develop one's personality ought to prevent.

A new right? No, just a name for a specific interpretation of existing ones

So, in view of electronic data processing the German Constitutional Court, hence, sculptured the right to informational self-determination as a special sub-area of the general right of personality (there are more of such sub-areas, e.g. the right to one's own picture, the right to be left alone or the right in the confidentiality and integrity of IT systems). Data protection laws in this view are rather indirect tools to ensure or at least foster informational self-determination (cf. Rouvroy and Poullet 2009: 53).

Moreover, a right to informational self-determination with its consequences on personal developments is more or less indirectly fostering a free and vivid democracy. Self-determination in this view, enabling the individual to act freely, is also a necessary precondition for a free democratic society. Hence, not guaranteeing the right to informational self-determination also has an impact on common welfare.

Both lines of reasoning refer to a phenomenon of informational self-determination that does not make the theoretical approach anything easier: Of course, humans are social life forms after all, evolving within social structures and communities, and one's personality is always based on and shaped by interactions with other individuals. So, information related to a person always fulfils the function of a picture of the "social reality" which cannot be laid solely into the hands of the person affected. Hence, limitations of the right to informational self-determination have to be made for the interest of third parties.

The last thought has two major consequences for the legal concept of a right to informational self-determination: First, the existence of this right in no way results in an encompassing ownership of all the information that is out there. It contains such information that relates to a specific, identifiable

person or that relates to facts or circumstances concerning an individual. The person affected by such information shall have the ability to determine who should know, collect or disclose this information and how it should be processed. But, if there is an interest in processing the data by a third party (another person, company, state body or the public), this interest has to be balanced against the right to informational self-determination. Informational self-determination, thus, is a concept carrying both individualistic values as well as the function to enable a free and democratic society.

Principles for data protection laws

A right to informational self-determination has important consequences for its implementation in law: Self-determination and autonomy are no tangible resources and they cannot be granted by the lawmaker. To provide for a right to informational self-determination, the lawmaker, rather, has to implement a legal framework within which an individual is – theoretically – able to determine the processing of one's data. The concept of informational self-determination as a right of self-determination aims at empowering and supporting people to actively use their right of self-determination. In order to constitute such actively exerted individual rights, therefore, the lawmaker needs to implement institutional, organisational and procedural rights.

What arise from this theoretical background are the main principles of modern data protection laws:

- The individual should have control over the decision whether data is collected, stored or processed. His consent is needed. Only in limited cases, where external interests outweigh the right to self-determination, should the collection, storage or processing be allowed.
- In cases where a person declares his consent to data processing, the individual has to be informed in advance about the type of data being processed and the purpose of processing. Without knowing the purpose of data processing, consent would lack its function that the person can oversee factual or potential consequences for his self-determination.
- To keep track of the relevant personal data, the individual must have the right to information, i.e. to access this information against third parties.
- To minimize risks for informational self-determination an organisational premise of data protection must be data security and minimisation of data collection and processing (data protection by design).

Information society: Challenging the underlying assumptions

During the last 30 years, enormous technological and societal changes have taken place, challenging at least some of the assumptions made by informational self-determination:

For one thing, information asymmetries, when it comes to collecting, storing and processing data, worsened, despite regulations. Consumption goods and their distribution get digital, services are offered electronically, customer retention strategies have spiked, all backed by huge ERP and CRM systems - let alone new services and business models made possible by the internet. This led to the present situation of "consent all over the place", where contract terms, terms of service and end user licence agreements usually include the user's consent to the processing of his data, often extending

beyond the sole purpose of fulfilling the contract or providing the service. Here, consumers' general inertia regarding such mandatory terms "is a strong and pervasive limitation on free choice" (Schwartz 2000: 823), and permits notices to become an alibi for "take-it-or-leave-it" data processing (ibid. : 825). Result is a habitualization of one-directional one-click consent, without (a) the possibility to say "no" and still being able to use the service and (b) consciously taking into consideration the potential consequences of each consent for the own development of a self-determined personality. It is more an uninformed or even negligent choice than a deliberate action. However, the concept of informational self-determination is based on the assumption that a person actually *wants to actively decide* on who collects what data for what purpose.

With the exorbitant success (here, from a social rather than from an economic perspective) of social networking services (SNS) another aspect of the underlying concept is challenged: People sometimes *want to publish* their personal data in social worlds. The important function of SNS, when it comes to self-display in peer-groups or in general public, cannot be underestimated. Creating and "tuning" one's perceived personality via SNS is an activity that is closely related to the possibility to freely develop his or her own personality autonomously. However, changing contexts and the underrated size of "public private spheres" in SNS also pose a threat for informational self-determination. In the end, these diffusing new spheres between public and private are raising the question whether the implications for the right to informational self-determination are still foreseeable for the individual in general: When the objective of the right is to decide about who knows what data, but the "who" isn't predictable anymore, the current situation at least undermines autonomous and terminal decisions due to the complexity or even obscurity of their consequences.

Third, the current concept of informational self-determination rests upon the expectation that the two most problematic counterparts of the right to self-determination are state bodies on one side and companies on the other side. While this assumption still seems to be right, another phenomenon has not been anticipated by the concept. Data processing is being done more and more by private individuals. SNS in this respect have to serve as examples. Sharing, liking, copying, forwarding or commenting on each other's posts always includes the processing of a third party's personal data – intentionally or incidentally. These social interactions elude the current notion of informational self-determination, as they usually fall within the sphere of necessary social interaction – like explained above – but nowadays tend to exceed traditional – framed and limited – social interaction. In practice, the increased data processing by laymen or private third parties also poses the question whether laws still aim at the right direction and whether they are written in the right language for the extended "target group".

Informational self-determination in current communication practices: Empowerment of those affected

It has become clear that the current challenges do not question the idea of informational self-determination in general. The idea remains a good one. However, it seems necessary to reinterpret the concept in view of the modern information society, filling it with life again in the right areas. As

personal information, personal and public communication and personal data become more and more intertwined, posing both risks to informational self-determination and fostering personal liberties in parallel, they should be considered together from a regulatory perspective, too. Especially in the intersection between information rights, information interests and personality rights, there is a new need for an information law that is granting freedom and limitations within one coherent framework, emphasizing the ambivalence of data handling for individual freedom, social interaction and public communication. Communication scientists already make use of the concept of informational self-determination, extending it towards an approach of "self-determination by informational means" in media literacy. In the field of SNS, this framework ends in a differentiation of activities into categories of "identity management", "relation management" and "information management" (cf. Paus-Hasebrink, Lampert and Hasebrink 2007: 2).

With ever more complex data processing possibilities and increasing amounts of data arising en passant, making it easier to process and analyse personal data, the objective of an appropriate interpretation of informational self-determination has to be to use the same modern technology to simplify the information and control possibilities of individuals when exerting their right, especially with regard to transparency, autonomy of decisions and the possible courses of action. Law, in this area, will meet its (national and theoretical) limits soon, once a potential risk materializes in practice, as information tends to diffuse quickly and irreversibly. Hence, regulation will have to focus on setting incentives for implementing structures and techniques that aim both at minimizing potentials for privacy risks ("privacy by design") and at maximizing the technical possibilities for the individual to protect his privacy in case of infringements ("privacy by tools"). Finally, new forms of governance have to be found in a global data processing environment to help implement such objectives: Multi-stakeholder approaches and new control instruments (e.g. community-backed information and control, informational regulation tools like transparency obligations, new forms of information obligations like icon-based privacy statements) might be the first steps to implement informational self-determination as a common global value ("privacy as an ethical standard").

References

Flaherty, D. (1990): On the Utility of Constitutional Rights to Privacy and Data Protection. Case Western Reserve Law Review 41, pp.831.

Hornung, G.; Schnabel, C. (2009): Data protection in Germany I: The population census decision and the right to informational self-determination. Computer Law & Security Review 25, pp. 84.

Kunig, P. (1993): Der Grundsatz informationeller Selbstbestimmung. Jura 1993, pp 595.

Paus-Hasebrink, I.; Lampert, C.; Hasebrink, U. (2009): Social Network Sites - Challenges for Media Literacy. EU Kids Online Conference June 2009. London. Available at

http://www.lse.ac.uk/collections/EUKidsOnline/Papers%20and%20abstracts/Online%20Opportunities%20and%20New%20Literacies/Paus-Hasebrink.pdf [29/02/2012]

Pitschas, R.(1998): Bedeutungswandel des Datenschutzes im Übergang von der Industrie- zur Informationsgesellschaft. In: Sokol (ed.), 20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?, pp. 35.

Rouvroy, A.; Poullet, Y. (2009): The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth et al. (eds.), Reinventing Data Protection?, pp. 45.

Schwartz, P. M. (2000): Internet Privacy and the State. Connecticut Law Review 32, pp. 815.

The Reform of the data protection legal framework

Panayota Boussis

The European Commission proposes a new, clear and uniform legislative framework, which will ensure a strong protection of the fundamental right to data protection throughout the European Union and at the same time, will strengthen the functioning of the Single Market.

Building trust in online environment: a challenge for the Commission

The phenomenal development of new technologies has an undeniable effect on the ever-increasing volume of personal data collected, accessed, used and transferred. By using smart cards, cloud computing or social networking sites, we leave digital traces at every "click" we make. At the same time, collecting and analyzing personal data has become a real asset for many companies of which the economic activities are mainly based on the analysis of the data of potential customers.

When disclosing their personal data, people are absolutely aware that their data will be processed. They feel however that they are not in complete control of them and they are concerned that their personal data may be misused. This lack of confidence in online services definitely affects the growth and the competitiveness of the digital economy within the European Union.

Building trust in the online environment seems essential to economic development. A reform of the current legislative framework was therefore required in order to ensure a high level of data protection, enhancing thus trust in online services and fulfilling the potential of the digital economy. This reform is even more important given the central role of personal data protection in the Digital Agenda for Europe and in the Europe 2020 Strategy.

Current Legislative framework: Directive 95/46/EC

The existing legislation at European level on personal data protection is the Directive 95/46/EC[4], adopted in 1995 with a double objective: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. Directive 95/46/EC has been completed by the Framework Decision 2008/977/JHA as a general instrument at Union level for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters[5].

Nowadays, we are facing new challenges for the protection of personal data, principally due to the technological developments. The scale of data sharing and collecting having increased considerably, the objectives and principles protected by the current legal framework need more than ever a strong and coherent protection. Indeed, the current legal framework has a main weakness: it has not

[4] COM(2010)171 final
[5] COM(2010)245 final

prevented fragmentation in the way personal data protection is implemented across the Union. Under Directive 95/46/EC the ways in which individuals are able to exercise their right to data protection are not sufficiently harmonized across Member States. Nor are the powers of the national authorities responsible for data in order to ensure consistent and effective application of the rules within the European Union. This fragmentation may lead however to legal uncertainty and as a result to the public perception that there are significant risks associated with online activity. Indeed, many Europeans consider that they are not properly informed of the processing of their personal data and they do not know how to exercise their rights online.

A stronger and more coherent data protection framework within the European Union is therefore essential. It would put individuals in control of their own data, reinforce legal and practical certainty for economic operators and public authorities and allow hence the digital economy to develop across the internal market

The right to protection of personal data is protected by Article 8 of the Charter of Fundamental Rights of the EU as a fundamental right. Likewise, the Treaty on the Functioning of the European Union (TFEU) establishes in Article 16 (1) the principle that everyone has the right to the protection of personal data concerning him or her and introduced a specific legal basis (Article 16(2)) for the adoption of rules on the protection of personal data.

This is on that basis that the Commission proposes a new legal framework on data protection. After assessing the impacts of different policy options, the European Commission proposes a strong and consistent legislative framework across Union policies, enhancing individuals' rights, cutting red tape for businesses, enhancing thus the Single Market dimension of data protection.

One aspect of the reform is the nature of the legal text. Data protection requirements and safeguards will be set out in a Regulation with direct application throughout the Union.

The proposed legal framework consists of two legislative proposals:
– a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and
–a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

The right to protection of personal data

The right to protection of personal data is established by Article 8 of the Charter and Article 16

TFEU as well as in Article 8 of the ECHR. According to the Court of Justice of the EU[6], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society. Data protection is closely linked to respect for other rights established by the Charter such as i.e. freedom of expression (Article 11 of the Charter); the rights of the child (Article 24) the right to property and in particular the protection of intellectual property (Article 17(2)); the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21).

Objectives of the reform

Putting individuals in control of their personal data

One of the priorities of the new legal framework on data protection is to allow individuals to exercise an effective control on their personal data. This rejoins the expectations of many Europeans who although they consider that disclosure of their personal data online is inevitable, they feel that they are not in control of their data since they are not properly informed of what happens to their personal information once disclosed. Often, as already mentioned, they do not know how to exercise their rights online.

The reform of the EU data protection rules will namely ensure the "right to be forgotten" by introducing an explicit requirement that obliges online social networking services to minimize the volume of users' personal data that they collect and process. The proposal foresees also an explicit obligation for data controllers to delete an individual's personal data if that person explicitly requests deletion and where there are no other legitimate grounds to retain it. Moreover, it is foreseen that the default settings shall ensure that data is not made public.

The individual's ability to control their data will be improved with the proposed Regulation, which will ensure that, when their consent is required, it is given explicitly and freely with a clear affirmative action by the person concerned.

In addition, the Regulation will strengthen the right to information so that individuals fully understand how their personal data is handled, particularly when the processing activities concern children. It will also guarantee an easy access to individual's own data and a right to data portability, i.e. a right to obtain a copy of the stored data from the controller and the freedom to move it from one service provider to another.

The new legal framework intends to reinforce national data protection authorities' independence and powers, so that they are properly equipped to deal effectively with complaints, with powers to carry

[6] Judgment of Court of Justice of the EU of the 9th of November 2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000

out effective investigations, take binding decisions and impose effective and dissuasive sanctions. It also aims at improving administrative and judicial remedies when data protection rights are violated. The new text foresees namely the possibility for qualified associations to bring actions to Court on behalf of individuals.

Enhancing of the accountability of the data processors

The aim of the reform proposed by the Commission is to strengthen individual rights, by informing them of the processing of their data and by allowing them to exercise their rights more effectively. The reform of the EU's data protection rules will oblige thus companies to strengthen their security measures to prevent and avoid breaches and to notify data breaches to both the national data protection authority – within 24 hour of the breach being discovered– and the individuals concerned without undue delay.

The Regulation introduces also the " Privacy by Design" principle to make sure that data protection safeguards are taken into account at the planning stage of procedures and systems. Moreover, the new text introduces for organizations involved in risky processing the obligation to carry out Data Protection Impact Assessments.

In addition, the proposed Regulation introduces the concept of "risky processing" and requires from data controllers to designate a Data Protection Officer in companies with more than 250 employees and in firms which are involved in processing operations which, by virtue of their nature, their scope or their purposes, present specific risks to the rights and freedoms of individuals.

Strengthening the functioning of the Single Market

The Commission proposes a clear and uniform legislative framework at European level, which will help to strengthen the potential of the Digital Single Market and promote economic growth and innovation. The chosen form of the legal text will put an end to the fragmentation of different legal regimes across the Member States and remove thus the obstacles to market entry. A Regulation directly applicable in all Member States will avoid cumulative and simultaneous application of different national data protection laws. This will definitely simplify the regulatory environment and as a result will cut red tape and eliminate formalities. This will particularly help micro, small and medium sized enterprises to which a special attention is given their considerable importance for the competitiveness of the European economy.

In addition, Commission proposes to further enhance the independence and powers of national data protection authorities (DPAs) in order to make them more effective. They will be given the possibility to carry out investigations, to take binding decisions and to impose effective and dissuasive sanctions. Moreover the Regulation will give the possibility to data controllers in the EU to deal only with the DPA of the Member State where the company's main establishment is located. Hence in case of violation of data protection, only the data protection authority where the company has its main establishment will be responsible for deciding whether the company is acting within the law or not. At the same time, the Regulation aims in ensuring a prompt, and effective coordination between national data protection authorities, by creating the conditions for an efficient cooperation between

DPAs, including the obligation for one DPA to carry out investigations and inspections upon request from another as well as the mutual recognition of each other's decisions.

Data protection in a globalized world: is it still possible?

What is sure is that it is a main concern for the Commission. Nowadays, only one "click" allow people to be in in different places in the world. That means however that personal data is being transferred across an increasing number of virtual and geographical borders and stored on servers in multiple countries. Besides, several companies offer cloud-computing services, allowing customers to access and store data on remote servers. This involves a real need for improvement of the current mechanisms for transferring data to third countries, in order to secure a high level of data protection in international processing operations and facilitate thus data movements across borders.

The Commission proposes therefore to establish clear rules defining when EU law is applicable to data controllers established in third countries. In addition, the Commission underlines the need to simplify and to strengthen the rules on international data transfers to countries. The Commission also suggests engaging negotiations with third countries – particularly EU strategic partners and European Neighbourhood Policy countries in order to promote high data protection standards worldwide.

Processing of data in police and criminal justice cooperation

The proposal of the Commission foresees also a Directive on the protection of individuals with regard to the processing of their personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

The introduction of a new legal basis (Article 16 TFEU) with the Lisbon Treaty allows the establishment of a coherent data protection framework ensuring a high level of protection for individuals' data, whilst respecting the specific nature of the field of police and judicial cooperation in criminal matters.

To ensure a high level of protection of personal data in that specific field, the Commission proposes a Directive, which will apply general data protection principles to police cooperation and judicial cooperation in criminal matters and provide for a minimal harmonization of criteria and conditions on possible limitations to the general rules, especially as regards the rights of individuals to be informed when police and judicial authorities handle or access their data.

Conclusion

Nowadays, people are aware that the protection of their personal data is a right. However they do not know how to ensure the respect of their right. When they are online even when they are only looking for an information online- they immediately realize that their data are processed but they do not know to what extend they are processed.

The reform of the legal framework on data protection will therefore first benefit those individuals by strengthening their data protection rights and their trust in the digital environment.

By its clarity and its coherence, the reform will furthermore simplify the legal environment on data protection helping thus businesses, but also the public sector significantly. This is expected to stimulate the development of the digital economy across the European Single Market, in line with the objectives of the Europe 2020 strategy and the Digital Agenda for Europe.

Conflict between the United States and the European Union with regard to data protection and privacy issues

Manon Steibel

This article explores differences between the U.S. and the EU related to privacy through two cases studies.

The digital age

These last fifty years, we are progressively entering into a new age: "the so-called digital age"[7]. The use of Internet has become more and more important over the years in such a point that living in our modern societies without Internet became improbable. Today, we are using Internet for all our activities: we communicate principally online, we shop online, we socialize online through a lot of social networks, and we keep informed about news online. This rapid expansion had as a consequence that an important amount of personal data is generated and the majority of them has been revealed by all of us through email and social networks like YouTube, Facebook, LinkedIn, Google's index. However, these personal data are often used without our agreement and are collected, analysed and stored. Indeed, our Internet travels are recorded in order to predict our consumer behaviour. Many companies are specialized in the area of the behavioral advertisement. However, there is a difference between collecting and tracking information with our agreement and these practices where the companies are putting cookies on our desktop[8].

This situation has raised concerns over privacy protection in an online environment. The protection of personal data is not a new concern but nowadays the privacy is affected by the new technologies in such a way that we can easily collect, store and market personal information. The policy-makers were alerted by these concerns. However, there is no common definition of privacy. This implies that each national government has its own conception of privacy and defines its policy in relation to the latter. Thus, conflicts between the different national policies may appear since the Internet has no geographical borders and its data flows freely. The social and cultural differences of privacy conception between the United States and the Europe and the conflict, which results from it, are a perfect example of this statement.

Clash between United States and European conceptions of privacy: Dignity vs. Freedom

In the United States, the right to privacy was established as a principle of common law in 1890 in an article written by Samuel Warren and Louis Brandeis for the *Harvard Law review*. They defined the right to privacy as "The right to be let alone". The right to privacy is conceived in the US law as an interest among others. There is no explicit mention to "privacy" in the U.S. Constitution or the Bill of Rights. However, the Supreme Court relied on several Amendments of the Constitution, in particular

[7] Terence Craig and Mary Ludloff, *Privacy and Big Data*, Editor Blanchette et Loukides, 2011.
[8] Id.

the fourth one, in order to develop this right to privacy. In the American privacy conception, the person and its home are the main subjects of this protection[9]. They are protected against unlawful intrusions such as unlawful search and seizure. In the U.S. system, the idea is that privacy is a tool against the government for limiting federal and state powers. In the U.S., the markets and self-regulation- not the law- are dealing with privacy issues[10], especially in the e-commerce area. In the USA, a complicated and segmented regulatory framework governs data protection, instead of a central privacy law, That regulatory framework is based on the consideration that privacy is a commodity and the consumer has to remain vigilant about their privacy.

Contrary to the U.S. conception of privacy, Europeans consider privacy, as a fundamental right and privacy protection is an obligation of the government towards its citizens. In Europe, the right to privacy is widely regulated in both national and supra-national level. Many European countries like Germany or Spain mention privacy in their Constitutions. At supra-national level, two important policies exist as regards data protection. The European Convention on Human Rights supports a right to privacy in its article 8 "*Everyone has the right to respect for his private and family life, his home, and his correspondence*". The European view of privacy is more focused on the preservation of the individual's honour and dignity even in the public sphere. The second supra-national regulation is the European Union Data Protection Directive[11], which establishes uniform provisions for the processing of personal information in the European Union. This directive aims at harmonizing the different national legislations in privacy matters, promoting the free flow of personal data within the European Union and setting a baseline of security around personal information wherever it is stored, transmitted or processed.

Politics of transborder dataflows in a transatlantic perspective: Safe Harbor Effect and Passenger Name Record

As an illustration of the conflict between the U.S. and the EU regarding privacy and data protection, this article is dealing with two case studies. First, the Safe Harbor Agreement which was concluded between the two parties to regulate the way that U.S. companies export and handle the personal data of EU citizens and secondly, the dispute between the two same actors related to the transmission of passenger name records in transatlantic flights.

As mentioned above, the European Union harmonized the legislations of Member States related to privacy and data protection in 1998. In accordance with Article 25 of the Directive, the transfer of personal data to a third country, which does not provide an adequate level of data protection, is forbidden. According to the European Union, the U.S. lacks adequate data protection standards. Therefore, in order to continue transatlantic business, the U.S. department of commerce and the

[9] Id.

[10] Lauren B. Movius and Nathalie Krup, *U.S. and EU Privacy Policy: Comparison of Regulatory approaches*, IJC 2009.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, p. 31

European Union concluded an agreement in 2000, the Safe Harbor Agreement. This agreement allows U.S. companies to transfer and to store personal information if they met the "adequacy standard" of the EU Directive. Safe Harbor stipulations require that: companies collecting personal data must inform people about the purposes for which they collect and use information about them; they must obtain permission to pass on the information to a third party; they must allow people access to the data gathered; data integrity and security must be assured; and a means of enforcing compliance must be guaranteed. The Safe Harbor agreement does not represent a piece of legislation but a self-certification. Indeed, U.S. companies can certify to the department of Commerce that they met the seven Safe Harbor principles. After more than ten years of existence, the Safe Harbor agreement is all but a success. Indeed, many companies took advantage of it and published misleading information about their privacy policies in order to obtain the certification. Furthermore, the Safe Harbor agreement imposes restrictions on data processing, which render the use of the Safe Harbor framework problematic in the U.S. discovery context[12]. Indeed, the EU Data Protection Directive, and the restrictions that it provides on transfers and processing, poses problems for litigants involved in U.S-EU trans-border litigation. Parties involved in U.S.–EU trans-border litigation may not be able to satisfy the discovery requirements of the Federal Rules of Civil Procedure without violating EU Data Protection Directive and will often choose to breach the European rules. Indeed, the failure to comply with the federal rules could lead to severe sanctions as important fines, prosecution for obstruction of justice and dismissal of claims.

The dispute between the U.S. and EU is always in progress with the announcement of the EU data privacy reform by the EU justice Commissioner Viviane Reding. The U.S. Department of Commerce has already circulated two informal notes with comments and criticisms on the proposals for a data protection Regulation and a Directive on data protection in the field of law enforcement. Many U.S. lobbies are trying to soften the rules in order to protect the interest of U.S. companies in the EU.

Another area of dispute between the U.S. and EU resulting from the different privacy conception and different regulatory approaches is the travel industry and the issue of Passenger Name Records (hereafter "PNRs")[13]. PNRs are information provided by passengers and collected by air companies for their commercial purposes. PNRs includes sensitive personal information including the name of the traveller, its address, its phone number, its family or business information, its credit card details but also information about an eventual physical or medical disease, and preferences about its travels. Most of major companies choose to outsource their PNRs to a Computerized Reservation System and any company offering services like hotels have access to the PNRs through this system. After the terrorist attacks of the 11th of September 2009, the U.S. government decided to use the PNRs in their fight against terrorism. The American Congress adopted "The Aviation and Security Act" which allows the U.S. Bureau of Customs and Border Protection to have access to PNRs. As a result, a conflict between the American Act and the EU Data protection Directive arose. This situation

[12] Carla L. Reyes, *The U.S. discovery- EU privacy directive conflict: constructing a three-tiered compliance strategy*, Duke Journal of Comparative and International Law, 2009.
[13] Id.

required negotiations between both sides. The U.S. government and European Commission reached an agreement in 2004, which provided that the transfer of data to U.S. authorities enjoys the adequate protection required by the EU Data Protection Directive. The agreement was concluded in order to prevent and fight terrorism and organized crime. However on 30 May 2006, the European Court of justice invalidated the U.S.-EU PNR agreement. A new PNR agreement was reached in 2007 with nineteen data types, which can be transferred to the U.S. government.

Within the framework of its new power under the treaty of Lisbon, the European Parliament adopted a resolution in 2010 requesting the re-negotiation of the existing PNR. In November 2011, the EU and the U.S. have initialled a new agreement on the transfer of passengers' data for flights from the EU to the US. According to Cecilia Malmström, EU Commissioner for Home affairs, the new agreement will ensure a higher protection of the EU citizens' privacy without questioning the agreement between the UE and the U.S. for the security. The new agreement is a legally binding text that reinforces police and law enforcement cooperation. Now, the U.S. authorities will be obliged to cooperate with EU authorities by sharing PNRs Data in order to prevent and fight terrorism and transnational crimes. The agreement will provide rules in favour of the privacy protection by ensuring that data can only be stored for a limited period and by introducing a depersonalisation of the data six months after the transfer to the U.S. The new agreement provides that passengers can obtain access to their data in order to correct or delete their PNR. They can also seek administrative and judiciary redress as provided under US law. Furthermore, now the total period of data storage will be limited to ten years with regard to transnational crimes, i.e. five years less than under the existing PNR agreement. A fifteen-years limited period of storage will be maintained for terrorism[14].

To conclude, these two case studies illustrate the different view of the Unites States and the European Union as regards privacy conception. On the first case, a compromise was reached in order to balance the economic interests of the U.S. and the mixed approach adopted by the EU combining economic interest and the privacy protection. It has to be noted that the U.S. were in a weaker position since they have important economic interests in Europe. In the second case, it was the "safety interest" which came into play against the protection of privacy[15]. In the context of PNR case, it was the European Union, which was in a weaker position. For this reason, it was decided to endorse to the U.S. position in order maintain the landing rights of European air companies in the U.S. The new PNR agreement should balance the safety interest and the protection of privacy.

[14] *New EU-US agreement on PNR improves data protection and fights crime and terrorism*, Europa press, IP/11/1368
[15] Andreas Busch, *The regulation and politics of transborder dataflows,* Conference, University of Bath, September 7th-8th 2006.

Who should have the last word, big industry or the regulator?

Paraskevi Kollia

The clash between multinational companies -with increasing lack of accountability and violations of the law- and the regulatory forces that ought to bring the situation under control is becoming central in our society, even if often citizens are unaware of it.

Introduction

Are modern societies based on the market economy a direct evolution of the traditional ones, where the public interest was the exclusive task of the public authorities (democratic or not)? The answer could be yes, if care for the public interest nowadays still was in the remit of the public imperium. Presumably, it still is. However, new uncontrollable forces, such as the new technologies and globalization and their rapid and powerful impact have revolutionized the passage to the market and overruled the classical concept of human rights, as the democratic relationship between citizens and authorities has been replaced by the triangle citizens-public authorities-market, without there being clear prevalence of the public authorities as protectors of citizens. Should this become structural, we would not speak about an evolution of society of values to a market society any more, but rather about a rupture of eternal so far concepts. Although it is too early to draw a final conclusion, it is rather timely to question ourselves and then decide consciously the direction our society should take. Two omnipresent examples illustrate the problematic and can help show the correct orientation. In any case, this will not happen by itself, it requires decisive intervention or conscious abstention by the regulators and the civil society.

Credit Rating Agencies and the "magic" of rating

The recent proposals of the EU Internal Market Directorate-General to publish new legislative measures both on regulating the Credit Rating Agencies' ("CRAs") methodology and imposing stricter accounting standards, tackle the crucial issue of the uncontrolled and subjective, often erratic, function of the said agencies and their disproportionate effect on the Internal Market.

The adopted by the Commission proposals[16] are, as expected, lighter in terms of strictness and supervision of the CRAs than the initial proposals by Mr. Michel Barnier, the Internal Market Commissioner. This has been justifiably attributed to intense lobbying; "Unchecked power and money is the big problem with credit rating agencies", said the president of the Party of European Socialists, Poul Nyrup Rasmussen.

[16] Euractiv.com, 15.11.2011, "Credit ratings suspension ditched under proposed rules"

Numerous incidents during the recent financial crisis have evinced the flawed way in which these agencies work; their actions have actually exacerbated the recession. The CRAs rated far too positively financial instruments (especially more complicated structured financial products), which were in reality "junk", and banks that were in reality going bankrupt. At the same time, they downgraded the Greek debt during negotiations on the country's bailout and also downgraded other Member States at a time when austerity measures were implemented all across the Euro zone.

The final straw, apparently, was the "mistaken" downgrading of France, which started making everyone wonder how much influence the CRAs have come to acquire over elected governments. These decisions have been criticized as inconsistent and unreasonable by EU politicians and Commission heads, and greater transparency and supervision on the CRAs was called for.

Not negligible is also the question of conflicts of interest; CRAs have no problem acting both as financial advisors to the issuer of the products, i.e. their clients, and subsequently rating these products.

Moreover, the lack of competition in the financial rating market results in an oligopoly model, due to extremely high barriers to entry in the relevant market (high reputation is the crucial element for this) and lack of comparability of ratings, which is detrimental to the consumers. Unfortunately, the originally to be banned large-scale- mergers in the market have now been allowed, due to the lack of support by the majority of the Commissioners.

Last but not least, overreliance of financial institutions on CRAs' ratings, the extreme effects such rating changes have on sovereign debts and the limited rights of redress for loss due to inaccurate ratings are all issues identified and correctly sought to be addressed by the EU legislature. It is now clear, the agencies need to undertake a sense of responsibility vis-à-vis the society.

The Commission may have turned down Mr. Barnier's initial suggestions for European Securities and Markets Authority ("ESMA") right to suspend rating sovereign debts for countries in special circumstances, e.g. negotiating bail-outs; the plan for an EU credit rating agency was also rejected, as presumably it would be too expensive and lacking credibility in relation to the other agencies.

The new pieces of legislation, however, will make it possible for CRAs to be sued for civil liability in case of intent or gross negligence, the burden of proof resting with the agency. This will increase accountability. Another positive measure is the obligation of institutions using the agencies to rotate among the firms every 3 years, thus increasing competition as well as independence. Investors are encouraged to not mechanically rely on the CRAs' ratings in making choices, but assessing the credit risk through internal risk management and rating models. Finally, the ESMA will acquire the power to review the methodologies CRAs are using and ensuring they comply with the legal regulatory standards.

The CRAs' response to the proposals is that they are "politically motivated and impractical, liable to damage the quality and independence of ratings, as well as inconsistent with the objective of stabilizing credit markets"[17]. It does not follow, however, that rotation will be counter-productive and decrease the ratings' quality. Independence is crucial, but it does not take precedence over the general interest; independence should not result in cannibalism, and this is what the European regulatory framework seeks to achieve, to impose better corporate governance on European banks and businesses. The question is whether it goes far enough.

The overreliance of the whole financial world on the ratings of three agencies is problematic; especially when these have shown that they can issue misleading ratings as they please and unduly influence the course of economy; yet, irrespective of that, as well as irrespective of the merits of CRAs, it remains a fact that their remit lies in the hard core of the public sphere and that their action shares the exercise of public power; consequently, CRAs cannot act on their own presumably following the rules of the market. The proposed legislation is definitely towards the right direction in submitting the agencies' analysis methods to scrutiny. It is a matter of time to see whether the agencies will comply with the regulator or whether more or maybe less affirmative action is needed. The bottom line is that actions that have such a tremendous impact on investors, borrowers, issuers and governments alike should be strictly regulated "for the prevention of disorder"[18] and the protection of the general good.

The boy who cried wolf: The case of Google

Google is no stranger to violations of privacy. So much ink has been spilt over its irresponsible and arrogant stance towards both the users of its services and any regulatory authority that has urged it to comply with legal standards of protection of privacy. This is all the more infuriating when the dominant position it has acquired in the market has come about in an overwhelming percentage through the handling of its users' personal data; at the same time, it keeps on assuring them that "all is well" when it very obviously is not. The inconsistency between its statements and its practices (i.e. constant flagrant privacy breaches) should finally be appropriately sanctioned.

Google has a market share of 95% in most EU Member States markets; so it should make sure it does not violate EU legislation on data protection (Directive 95/46/EC) and competition (Art. 101-102 TFEU). It is also crucial that all companies operating in the EU show utmost respect to the Charter of Fundamental Rights of the European Union (inter alia, right to respect for one's private and family life, home and correspondence and the protection of personal data).

[17] Electronic version of "The Telegraph", 15.11.2011, "EC's Barnier forced to put off credit ratings ban"
[18] Commission impact assessment SEC(2011) 1354

It is clear from Google's practices that we cannot rely on its good will; without contesting its input in the academic, political and social life in general as the unprecedented phenomenon it is, its practices allow concluding that it acts hypocritically, lacks credibility and, frankly, has made great progress in being viewed as Big Brother. The increased competition with its countervailing force in advertising, Facebook Inc., is quickly leading to the emergence of the "transparent user", i.e. Internet users constantly bombarded with targeted advertisements.

It is true that a systemic element of the company is to have access to personal data in order to "organize it" and make users' access to it as efficient and convenient as possible; but at the same time it is taking immense advantage of its users through the demographic data it collects, which is perfect for targeted advertising. Users do not always realize that they are not Google's clients –as the services are for free-, rather they are its "bait", with which it allures its actual clients, advertisers, and gains overwhelming market power. As a result, Google plays by its own rules in the market, due to the amount of information it possesses and exploits, and it does not comply with legal standards; advertisers face increased costs and undertakings have to comply with Google's rules in order to survive. Moreover, it often displays its own products or services on top of others, thus unfairly limiting competition; this has a big effect on the market, due to the search engine's popularity. The European Commission is currently investigating an abuse of its dominant position in Europe.

As eloquently put by John Simpson, advocate for Consumer Watchdog *"Once again Google has demonstrated a lack of concern for privacy. Its computer engineers run amok, push the envelope and gather whatever data they can until their fingers are caught in the cookie jar. Then a Google executive apologizes, mouthing bafflegab about how privacy matters to the company. The takeaway from this incident is the clear need for government oversight and regulation of the data all online companies gather and store."*

The challenges brought by Google to regulators and consumers alike are immense. Some users may not realize it –most do, thankfully- but Google is committing identity theft of the worst kind. It is critical that the public be more educated and aware of the intricacies of the Internet, beginning from simple steps, such as personalizing the default settings of a service in case it breaches their rights.

Additionally, data minimization[19] is undeniably the way to reduce such flagrant privacy breaches. Search engines should be more privacy-friendly and in no case store data after the search is over. Explicit, informed consent should be a prerequisite of any change in privacy policies or any storing or sharing of personal data.

But above all, the regulators must once and for all show Google that if it does not respect its users' privacy, sanctions will be enforced. Citizens have placed their trust upon the company, and now it is

[19] One of the principles in the Resolution on Privacy Protection and Search engines, London, 2nd-3rd November 2006, 28th International Data Protection and Privacy Commissioners' Conference.

crystal-clear that Google abuses it. Users now "pay" the free services or information by disclosing their personal information. The unparalleled power of the company has negative results for everyone except its own wallet; the public should be given the chance to take position, as surveys show that it is increasingly worried about the misuse of its data. The protection of EU citizens' fundamental rights should not only stay on paper.

Conclusion

Since the outset of the modern societies originating from the Greek democracy the value of the human being, the citizen, was out of any negotiation. If citizens managed to limit the absolute rulers, there is no excuse why they could not limit today's multinationals. Yet, in a democratic system this is the task of the regulators. And if the context has become too complex, the principles on which the EU is based are simple and clear-cut: they have to be unconditionally applied.

Pappas & Associates
Attorneys at law

Do you want a cookie?

by Damien Thavard

This is the question that - according to the current European rules- online advertiser networks should compulsory ask you before tracking your Internet browsing. It seems however that industry is reluctant to ask it, favoring rather the possibility for the users of an opt-out from online behavioral advertisement networks.

Online Behavioral Advertisement

Online behavioral advertising entails not only the tracking of users when they are surfing the Internet, but also the creation of profiles over the time, which are later used for advertising purposes. This technique is fruitful for both advertisers, who focus on people interested in their products, and customers, since they receive advertisements in connectin with their interests. This marketing practice implies however an intrusion into Internet users private life, since building such profiles implies the tracking, storing and processing of the data resulting from their Internet behavior.

The main tracking technology used to monitor users' behavior over the Internet is based on tracking cookies. A cookie is a short alphanumeric text stored in the user's computer. Such a cookie is placed in a computer when the user accesses for the first time a web-site, which is part of an ad-network. The cookie enables this network to recognize a former visitor who returns to a website (or to any other web-site partner of the ad-network). Those data are stored by ad-networks in order to build user's profiles. These profiles can be predictive, by comparing individual browsing with collective behaviors, or explicit when tracking technologies are combined with personal data provided by users, for instance when the ad-network provider is also providing other services requiring registration.

European legislative framework

At European level, two directives cover this commercial practice. The first one is the ePrivacy directive (directive 2002/58), and the second one is the Directive 95/46/EC relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The ePrivacy directive and specifically its article 5(3) is the most relevant text concerning the online behavioral advertising practice. Indeed, this article states that "*Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*". This article clearly establishes that in

order to have access to user's information, his consent is requested, and this consent has to be given after the user has been provided with clear information regarding the purpose of the data collection.

Directive 95/46/EC is also applicable for the processing of the collected data, notably as regards the quality of the data, or data's subjects' rights such as access, erasure or right to object. The current bone of contention between industry and privacy protection authorities is however the application of article 5(3). Indeed, the current practice of the industry is based on a self-regulatory initiative, putting forward the freedom of choice of the user instead of its prior consent.

Industry initiative

In April 2011, relevant actors of behavioral advertising have adopted a self-regulatory Best Practice Recommendation on online behavioral advertising (OBA). The adoption of this code of conduct followed the examination of the commercial practice on both sides of the Atlantic. In 2009, the European Union adopted the revised version of the ePrivacy Directive, and especially the new formulation of article 5(3) setting prior consent as the new rule while at the same time the Federal Trade Commission issued a report on OBA principles in which companies are requested to obtain affirmative express consent before collecting data for behavioral advertising.

The answer of industry is based on the freedom of choice of the user. Basically, the user has the choice trough a dedicated website to choose which ad-networks cookies he accepts or not. This means that the user can opt-out from the behavioral advertising system. The main concern with this concept is that it is completely the opposite of the current European legislation. Indeed, instead of asking user's consent prior placing a cookie on his computer and giving him relevant information on this issue, ad-networks offer the possibility to an individual to opt out from OBA, without even informing him clearly of this possibility while first placing the cookie.

This is a major issue. Indeed, one of the industry argument is that pop up screens are the only way to receive consent, and that such screens would be a nuisance for users who would have click trough multiple consent pop-ups. While there are multiple ways to obtain consent other than pop-ups (like splash screen or a static information banner) this statement does not take into account that when the user has made his choice and has given his consent or refusal there is no need to ask him again. The dedicated website allowing a user to opt-in or out, after having given his consent or having refused to place a cookie is interesting, making this choice non-definitive, and is a good supplement to the prior consent principle. However, it cannot replace the user prior consent since this would not comply with the ePrivacy directive.

The way forward

It is clear that OBA practices do not currently comply with the ePrivacy Directive. Although industry has been informed by the "article 29 Working Party" (the European advisory body regarding data protection made of representatives from members States competent authority, EU institutions and bodies and the European Commission), there are no current changes in this practice.

Next months will probably be decisive, for the settlement of this issue, especially at a time where the French data protection authority is investigating, after the invitation of the article 29 WP, the new Google privacy policy, one of the main operator in the field of OBA.