THE 7TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

EU and US Data Protection Reforms. A Comparative View

Gabriela Zanfir[1]

Abstract: This research makes a comparative analysis of two significant reform projects in data protection legislation, proposed in early 2012 in the EU and the US, in order to identify the common philosophies and also the main differences between them. Its outcomes are important as transatlantic data transfers are exponentially increasing and their main actors need to know what to expect from both legal regimes. The paper builds on a ground zero, as both reform projects were made public in late January – respectively late February, so such a comparison can only refer to researches made prior to the announcements regarding the general concepts of privacy and data protection in the European and American view. The main method employed is comparative observation. The results show that EU and US legislations start using the same language regarding data protection law – by the legal definitions proposed and main principles implemented, while still keeping significant differences. Academics and researchers will have a starting point for future comparative analyzes in a legal field which enjoys a lot of attention from lawmakers all over the globalized world. The paper focuses on very recent legal developments, which need throughout analysis in order to make them functional in practice.

Keywords: privacy; EU-US data transfers; legal definitions; privacy principles

1. Introduction

Privacy and data protection are a main concern for lawmakers of properly safeguarding human rights and democracies. Living in a Surveillance Society is already a fact of the modern world and not only an Orwellian product of imagination[2]. Thankfully, the democratic mechanisms keep the Surveillance Society in a framework of respect for human rights. Among such mechanisms, the most important is the regulation of the protection of privacy and personal information. A recent study discovered that the total number of new privacy laws globally, viewed by decade, shows that their growth is accelerating, not merely expanding linearly: 8 (1970s), 13 (1980s), 21 (1990s), 35 (2000s) and 12 (2 years of the 2010s), giving the total of 89 (Greenleaf, 2012). The phenomenon began in Europe, Germany being the first country which provided for a data protection law, but only in one of its regions – Hasse, in 1970. Several countries soon followed the model: Sweden, Denmark, France.

The European Union's jurisdiction became the leading global defendant of personal data, imposing a minimum standard of protection to countries that want to engage in data transfers with European entities. And one of the countries that do not provide a minimum degree of compliance is the United States of America. Hence, the two entities agreed upon a procedure called The Safe Harbor principles, which allow processors to make transatlantic data transfers. In early 2012, both countries made official announcements regarding data protection reforms. The European Commission published the proposed regulation for data protection on January 25 and the White House published the Consumer Privacy Bill of Rights a month later.

[1] PhD student, Assistant Researcher, Faculty of Law and Administrative Studies, University of Craiova. Address: 13 A. I. Cuza Str., Craiova 200585, Romania, Tel.: +40 251 414398, fax: +40 251 411688, Corresponding author: gabriela.zanfir@gmail.com.

[2] See 'A Report on the Surveillance Society' for the UK Information Commissioner, by the Surveillance Study Network (September 2006).

This paper will compare the two legal developments, underlying first the fundamental difference between privacy protection in EU and US which originates in philosophy. The paper continues with a general view on both reform projects, a comparison of the legal language used, focusing on the definition of personal data, followed by conclusions.

2. Different Philosophies of the Protection of Privacy

2.1. Europe: Privacy Protected as Dignity

Privacy and data protection are regulated different in the European Union and the United States. The EU centrally supervises the private sector's use of personal data, whereas the US regulation of the private sector is minimal. These differences emanate from distinct conceptual bases for privacy in each jurisdiction: in the US, privacy protection is essentially liberty protection, *i.e.* protection from government, while for Europeans, privacy protects dignity or their public image. (Levin & Nicholson, 2005). For instance, in Germany, for instance, on the basis of the current case-law from both the Constitutional Court and the Supreme Court, five broad-ranging protected personality interests developed under art. 823(1) BGB[1], with their own specific preconditions and sub-categories: (1) the protection of privacy; (2) the right to one's own image; (3) the sphere of publicity or the right to identity; (4) the right of informational self-determination (right to one's data); and (5) the protection of dignity, honour and reputation (Brüggemeier, Ciacchi, & O'Callaghan, 2010).

They are all rights to control your public image, rights to guarantee that people see you the way you want to be seen. They are, as it were, rights to be shielded against unwanted public exposure – to be spared embarrassment or humiliation, and, as such, the prime enemy of our "privacy", according to this view, is the media, which always threatens to broadcast unsavory information about us in ways that endanger our public dignity (Whitman, 2004). See, for instance, the famous case of Caroline of Monaco (Von Hannover v. Germany, 2004), where the European Court of Human Rights ruled that the publication of photos of the princess while she was engaged in private activities, alone or accompanied, in public spaces, such as parks, is a breach of Article 8 of the European Convention of Human Rights. Previously, the German courts had decided that the private life of the princess was not protected by Article 8, as she was a public figure.

2.2. America: Privacy Protected as Liberty

America, by contrast, is much more oriented toward values of liberty, and especially liberty over against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: it is the right to freedom from intrusions by the state, especially in one's own home (Whitman, 2004). Moreover, the US Constitution does not provide for a distinct right to privacy. This is why the protection of one's privacy is reconstructed as a puzzle in a quilt of statutes: The Right to Financial Privacy Act, The Identity Theft and Assumption Deterrence Act, The Cable Communications Policy Act, The Telecommunications Act of 1996 and even The Videotape Privacy Protection Act.

Previous research has shown that the absence of a constitutional right to privacy has two main effects. The first one is that the US piecemeal approach will result in various privacy-protecting acts clashing with well-established constitutional rights, and, as a result, their protection of privacy will be watered down (Levin & Nicholson, 2005). The second one is that the US Constitution with its supporting body of jurisprudence does not provide adequate privacy protection, especially in the light of continuing technological development (Levin & Nicholson, 2005).

Therefore, a Bill of Rights containing general guidelines for the protection of personal data is more than welcomed, especially that its content is approaching the European view on data protection. The

[1] The German Civil Code.

next section will analyze the general framework of the two reforms proposed recently by the EU and the US.

3. A General View on the Reform Projects

3.1. Scope and Objectives

Currently, the protection of personal data is regulated in the EU by Directive 95/46 on the protection of the individual with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive or DPD). This directive was adopted in 1995, when internet was living its infancy, less than 1% of the Europeans using the internet at that time (Reding, 2012). The general framework of the reform has as starting point the technological developments and the need to protect the individual in this context. The EC argues that "Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities". (European Commission, 2012). As such, we understand that the main purpose of the regulation is to effectively protect the individual from intrusions in his or her private life, highly accentuated by the developments of IT systems.

The regulation itself defines its material scope in Article 2(1) – "the processing of personal data, wholly or partly by automated means, and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system". Hence, the scope is broad and the main limitation is that the regulation only applies to natural persons, in that it protects their fundamental rights and freedoms, as stated in Article 1(2). The main accomplishment of the proposed regulation is the enhancement of the procedural, specific rights individuals have regarding the fair processing of their personal data: new rights are introduced and the existing ones are consistently developed. For instance, the "Rectification and erasure" section of the Data Protection Regulation (DPR) proposal is a part of Chapter III "Rights of the data subject" and it encompasses Article 16 – *the right to rectification*, Article 17 – *the right to be forgotten and to erasure* and Article 18 – *the right to data portability.* It should be noted that the right to be forgotten and the right to data portability are an innovation. All of these rights are provided in order to enhance control by individuals over their own data.

The US Consumer Privacy Bill of Rights (CPBR), on the other hand, is concentrating on the commercial aspect of the data protection and privacy debate. In the official document published by the White House containing the framework "Consumer Data Privacy in a Networked World" (White House, 2012), the Administration explains that "Privacy protections are critical to maintaining consumer trust in networked technologies. When consumers provide information about themselves - whether it is in the context of an online social network that is open to public view or a transaction involving sensitive personal information - they reasonably expect companies to use this information in ways that are consistent with the surrounding context". The discourse is evidently guided towards the economical, commercial spheres and not clearly towards the broader purpose of human rights protection. At the centre of this framework stands the Consumer Privacy Bill of Rights, "which embraces privacy principles recognized throughout the world and adapts them to the dynamic environment of the commercial Internet" (White House, 2012).

Another important component of the framework is the invitation launched to private stakeholders to adopt codes of conduct, based on the rules contained by the Consumer Privacy Bill of Rights (see, also, section 3.2).

The Administration observed that one of the elements the current piecemeal privacy framework lacks is "a clear statement of basic privacy principles that apply to the commercial world and a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models". This is the reason why the CPBR comprises seven principles

developed around basic rights individuals enjoy in relation to the protection of their personal data (see section 4.2).

3.2. Enforceability

EC chose to implement the data protection reform through a regulation. According to Article 288(2) of the Treaty on the Functioning of the European Union, a regulation is "binding in its entirety and directly applicable in all Member States", in contrast with a directive which is binding only as to the result to be achieved upon each Member State to which it is addressed, but shall leave to the national authorities the choice of forms and methods. Therefore, the rules provided in the DPR will directly apply in the legal orders of the Member States, without being implemented by national laws.

This was not the case with the Data Protection Directive. The different means of implementation chosen by the Member States led to significant differences in the protection of personal data throughout the EU, which caused legal uncertainty and a widespread public perception that there are significant privacy risks associated notably with online activity. Therefore, the choice of a regulation instead of a directive to implement the data protection reform is a premise of a more coherent data protection policy, of strengthened legal certainty and of a more effective protection of personal data inside the EU.

The Consumer Privacy Bill of Rights is not directly enforceable. It is "a guide for the Administration to work collaboratively with Congress on statutory language" (White House, 2012). Technically, the White House Administration is calling the US Congress to pass legislation that applies the principles contained in the CPBR to "commercial sectors that are not subject to existing Federal data privacy laws". Which means they will not unify the very decentralized current legislation, but will provide for concrete guidance to future legislation. The function of the rights provided in CPBR will also be active in the creation of future code of conducts. "The Federal Government will play a role in convening discussions among stakeholders - companies, privacy and consumer advocates, international partners, State Attorneys General, Federal criminal and civil law enforcement representatives, and academics - who will then develop codes of conduct that implement the Consumer Privacy Bill of Rights."

In the next section we will compare briefly critical legal concepts used by the two reform projects, to conclude that European and American privacy at least have started to use the same language.

4. The Legal Language Used

4.1 Definition of personal data

Delimiting the concept of the certain kind of information that legislations such as the ones being analyzed in this paper protect is of vital importance for the implementation of privacy laws. Recently, the results of a research completed in America showed that "information privacy law rests on the currently unstable category of personally identifiable information (PII). Information that falls within this category is protected; information outside of it is not" (Schwartz & Solove, 2011). The CPBR makes the "personally identifiable information" a stable concept, at least as far as consumer law is concerned. Moreover, the notion can easily be adopted by other sectors, now that it is legally defined.

The first statement of the CPBR is that "The Consumer Privacy Bill of Rights applies to personal data, which means any data, including aggregations of data, which is linkable to a specific individual".

The first observation is that the "personally identifiable information" is replaced with "personal data", a term used in the EU data protection law.

The second observation is that the concept of personal data is very similar to the one used in the EU: "any information relating to an identified or identifiable natural person" (Article 2a DPD). The DPR

introduces a renewed definition – "any information relating to a data subject" (Article 4(2)) and a data subject is "an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person".

The amount of details considered in the EU definition of personal data is explained by the significant role the delimitation of personal data has in the application of the law. Especially when "technologists can take information that appears on its face to be non-identifiable and turn it into identifiable data" (Schwartz & Solove, 2011) in the context of a fallen myth of anonymization (Ohm, 2010).

4.2. Principles

The DPR sets out the principles relating to personal data processing in Article 5, stating that personal data must be: a) processed lawfully, fairly and in a transparent manner in relation to the data subject; b) collected for specified, explicit and legitimate purposes; c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data; d) accurate and kept up to date; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes; f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of the regulation.

Most of these principles correspond to those in Article 6 of Directive 95/46, but they are renewed with the transparency principle, the clarification of the data minimization principle and the establishment of a comprehensive responsibility and liability of the controller. Chapter III of the Regulation is dedicated to the "Rights of the Data Subject" and it comprises 10 detailed articles which technically transpose the principles stated above.

The CPBR enforces seven rights each corresponding to one principle. „Individual control" gives the right to consumers to exercise control over what personal data companies collect from them. „Transparency" presupposes a right to easily understandable and accessible information about privacy and security practices. „Respect for context" means consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. „Security" is referring to the right to secure and responsible handling of personal data. „Access and accuracy" provides the right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate. „Focused collection" means consumers have the right to reasonable limits on the personal data that companies collect and retain. And, last, „Accountability" gives the right to consumers to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

Comparing the two frameworks we can find significant common concepts, which can be summarized in three main ideas: 1) the individual enjoys an enhanced control over the collection and processing of data, which implies consent, intervention and transparency; 2) the purpose and time limitation of data processing; 3) responsibility and accountability of the data processor.

The differences remain in several aspects. One of them concerns the entity which processes data and is accountable under the law. While CPBR is only referring to "companies", DPR is referring to "controller", which can be "a legal person, public authority, agency or any other body". Another difference is the legal certainty implied by the two provisions in general: while the DPR is specific,

maybe even too detailed, the CPBR, faithful to the idea of a bill of rights, is more general, leaving a lot of room for interpretation.

5. Conclusions

Even though their bases are fundamentally different, EU and US legal protection systems of privacy in general and informational privacy in particular found common denominators to start converging from. The EU data protection reform is a natural development of existing law, after two decades of evolution, while the US set of principles is a cornerstone for a coherent, unified legal protection system of privacy.

Both developments have in common the need to provide accountable and effective safeguards for individuals faced with the rapid evolution of technology. Both reforms envisage a more protected individual and a more responsible data controller or data processor. Even though they use completely different mechanisms to achieve these goals, at least they count on similar concepts.

The most significant difference between the reform projects remains the narrow scope of the Consumer Privacy Bill of Rights compared to the broad scope of the proposed data protection regulation. The first one only applies to commercial relations – the one who is being protected is "the consumer" and not "the individual", and the one accountable for breaching the consumer's legal safeguards can only be a "company". Nevertheless, the principles established for this specific domain can easily be taken into account for several other sectors.

6. Future Work

This paper is evidently only an introductory work and it can be continued at least in two directions. First, a study on circumscribing each principle stated in the Consumer Privacy Bill of Rights to certain mechanisms or provisions already implemented or soon to be enforced in the European Union. In this way, a more accurate correspondence can be made between the legal systems protecting personal data. This could also be a support for future US legislation and private codes of conduct. At the same time, the EU stakeholders could learn some lessons from the pragmatic way US Administration views informational privacy. Second, a research on how the CPBR could be implemented in the US legal system would be very interesting and also useful for the lawmakers and the private entities that are strongly encouraged to adopt codes of conduct.

7. Acknowledgement

This work was supported by the strategic grant POSDRU/CPP107/DMI1.5/S/78421, Project ID 78421 (2010), co-financed by the European Social Fund – Investing in People, within the Sectoral Operational Programme Human Resources Development 2007 – 2013.

8. References

Brüggemeier, G., Ciacchi, A. C., & O'Callaghan, P. (2010). *Personality Rights in European Tort Law.* Cambridge University Press.

*** Comission Staff Working Paper. (2012). Impact Assessment on the proposed Regulation, SEC(2012) 72/2.

Greenleaf, G. (2012). Global data privacy laws: 89 countries, and accelerating. *Queen Mary University of London, School of Law Legal Studies Research Paper* .

Levin, A., & Nicholson, M. J. (2005). Private Law in the United States, the EU and Canada: the Allure of the Middle Ground. *University of Ottawa Law and Technology Journal* , 357-395.

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* , 1701.

Reding, V. (2012, January 25). Public statement on the occasion of the press-conference organized after publicly launching the content of the data protection reform in 2012. Brussels.

Schwartz, P. M., & Solove, D. J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review* , 1814.

Von Hannover v. Germany, Application no. 59320/00 (European Court of Human Rights June 24, 2004).

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal* , 1151.

*** European Commission. (2012, January 25). COM(2012)11, 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. European Commission.

*** White House. (2012, February). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.