AN APPROACH TO A NEW AGREEMENT FOR EU/USA TRANSANTLANTIC PERSONAL DATA FLOW: AMERICAN TECHNOLOGY AND EUROPEAN LAW IN CONFLICT

Professor Rosa María García Sanz, Professor of Constitutional Law

University Complutense Madrid, **Spain**

ABSTRACT

The European Union (EU) and the USA have two very different models of personal data protection (European terminology) or information privacy law (American terminology). EU law has a defined and clear concept of personal data and a general law to protect this fundamental right. Meanwhile, the USA does not have a uniform definition of information privacy or personally identifiable information (PII); and it has only some sectorial laws to protect privacy in some markets.

Personally identifiable information is one of the most central concepts in information privacy regulation. The scope of privacy laws typically turns on whether PII is involved. At the same time, there is not a unique concept in US law for information privacy. Moreover, computer science has shown that in many circumstances non-PII can be linked to individuals, and that de-identified data can be re-indentified. In some way, then, we can say that the European law is applicable to almost all information on the Internet. And in some way, too, we can say that American technology uses data to establish its markets and services. These widely divergent positions present a difficult point from which to start looking for an agreement.

In addition, some legal categories of the European Law—General Data Protection Regulation (GDPR)—are not negotiable under contracts. Because of their inalienability they cannot be traded away by the free will of individuals, which complicates the mutual relationships between the two continents.

After breaking the SAFE HARBOR (after the SCHREMS EUROPEAN COURT DECISION Sept. 23, 2015, in CASE C-362/14) and under the New Agreement PRIVACY SHIELD FRAMEWORK 2016, new problems arose. Also, it cannot be forgotten that the prospects of the Internet of Things (IoT) and Artificial Intelligence (AI) are introducing new technologies that challenge the present laws and concepts.

These problems are asking for harmonized solutions that reflect cooperation of laws and policies for both sides of the Atlantic. This is necessary in order to continue with the traditional commercial relationship between Europe and North America and to work together against the terrorism threat. This paper will examine possible departure points, criteria and perspectives to find an approach based on the European Law (GDPR) and the US regulations and policies.

Keywords: Personal data protection law, information privacy law, privacy, Internet privacy, right to personal data

INTRODUCTION

The European Union (EU) and the USA have two very different models of personal data protection (European terminology) or information privacy law (American terminology) (See PAUL SCHWARTZ AND DANIEL SOLOVE).[i] EU law has a defined and clear concept of personal data and a general law to protect this fundamental right. Meanwhile, the USA does not have a uniform definition of information privacy or personally identifiable information (PII); and it has only some sectorial laws to protect privacy in some markets. Although the European Personal Data Protection Law[ii] does not apply to specific provisions of the common foreign and security policy or to the processing of personal data when it is about "public security" matters (GDPR art. 2.b.d), the American companies established in the EU allowed the American Government to get access to personal data without consent and to transfer them for different purposes from what the data subject had given consent (see SCHREMS EUROPEAN COURT DECISION Sept. 23, 2015, in CASE C-362/14 or "the disclosure of classified documents by Edward Snowden in 2013"),[iii] based on the aim of terrorism prevention.

After breaking the SAFE HARBOR, in the SCHREMS EUROPEAN COURT DECISION Sept. 23, 2015, in CASE C-362/14), the European Court of Justice (ECJ) held that the Safe Harbor did not provide an adequate level of protection because EU citizens were exposed to the US mass surveillance without limitation or guarantees. And under the New Agreement PRIVACY SHIELD FRAMEWORK 2016, new problems arose. An example of this can seen in the poor implementation of the Privacy Shield Principles by American companies, or in the case of Facebook where they provided misleading information to the European Union Commission during the approval process for the acquisition of Whatsapp (2014). As a result, the European Commission fined Facebook (May 18, 2017). Even more, on Nov. 13, 2014, Facebook announced a global revision of its data policy, cookie policy and terms. Following this announcement, a Contact Group was created at the European Union level with the Data Protection Authorities (DPAs) of The Netherlands, France, Spain, Hamburg and Belgium. The members of the Contact Group have initiated national investigations, relating to, amongst others, the quality of the information provided to users, the validity of consent and the processing of personal data for advertising purposes. Three of the members publish results on May 16, 2017 (France, Belgium and the Netherlands).

On the other hand, the worlds Internet of Things (IoT) and Artificial Intelligence (AI) are introducing new technologies that are challenging the present laws and concepts. Public and private sectors from both continents are touching a turning point where it is becoming critical to find some understanding between private businesses and governments' actions against terrorism, observing the rule of law and fundamental rights. The rigid limits of law can be overcome by good politics and policies between the USA and EU.

WHY A CONFLICT?

The European Union accuses the USA of technological imperialism. And, in turn, the USA accuses the EU of law imperialism. A starting point for understanding this dynamic is that European personal data law serves the individual in contrast to American information

privacy law that serves the marketplace. Under European Data Protection Law (GDPR), the central concept of "personal data" ('personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person)[iv] means that every piece of information on the Internet becomes personal data and therefore every piece of data falls under the scope of the GDPR. In addition, everything on the Internet is data (information or content). As previously mentioned, personally identifiable information is one of the most central concepts in information privacy regulation; the scope of privacy laws typically turns on whether PII is involved. But, at the same time, there is not a unique concept of information privacy in American law, and even in other countries, which complicates a consensus agreement (see DEIRDRE MULLIGAN).[v]

Another issue is that American companies use data to establish its markets and services. This makes it difficult to be anonymous on the Internet. For instance, individuals cannot make or receive a cell phone call without having that information tracked by the carrier; or Internet communications require the use of IP addresses that can be logged. Thus, there is little "voluntary" surrender of privacy in an electronic communication. Moreover, computer science has shown that in many circumstances non-PII can be linked to individuals, and that de-identified data can be re-indentified (see HELEN NISSENBAUM. [vi] The "promise" of avoiding the Regulation by anonymity has disappeared. Technology has defeated such possibility. But the problem is not just the speed at which the technology is advancing, though that is considerable.

The more profound problem is that some of the core principles that serve as a solid guide in today's privacy debates do not easily translate to an Internet of Things (IoT) world.[vii] The importance of business models and partnerships cannot be over emphasized in this world. Probably, the industry will work together in partnership to achieve goals. A starting point for the value chain will be to arrive at the appropriate business model for IoT; it will need to be based on partnerships and collaboration. That collaboration can involve different countries, continents, it can even be global. At each step along that value chain there are firms that make things; firms that provide services; firms on the periphery whose auxiliary inputs support the main value creation system (insurance, IP protection); and others. IoT has a very complex value chain due to the fact it impacts a large number of processes. And, in terms of personal data protection, that means firms collecting, processing, sharing and transferring data all the time, and, probably, without expectations of " individual consent" at every step and element along the value chain because of the technology's design. This problem seems to affect more EU law and its fundamental right to privacy than the USA information privacy law model. The American law starts with a principle of free information flow and permits the processing of any personal data unless a law limits the processing of personal data.

TIME FOR POLITICAL DECISIONS

The "irreconcilable" positions from both sides of the Atlantic are calling for a new approach based on politics and policies. Although fundamental rights are not negotiable, it is still possible to try a new common understanding of "information privacy" (American terminology and model) or "personal data protection" (European terminology and model). The aim will need to be finding an understanding that assures the essential content of the fundamental right and is able to deal at the same time with a digital context world in a more flexible way. That understanding brings a new approach that involves individual principles and rights over their personal data. Some legal categories of the European Law—General Data Protection Regulation (GDPR)—are not negotiable under contracts. Because of their inalienability they cannot be traded away by the free will of individuals, which complicates the mutual relationships between the two continents. Notwithstanding, the GDPR offers some avenues to Governments for finding solutions without betraying the essence and inalienability of those principles and rights. There are findings and articles that provide exceptions, exemptions, derogations and restrictions based on the "public interest", "legitimate interest" or "national security", and some rules in order not to apply the GDPR (material and territorial scope). Art.23 gives a general direction about: "1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard."

The opposite, without an agreement, means that EU closes its marketplace for American products and services and the US is not interested in the markets where the European law is applied (and that means more than EU countries). In addition, this "divorce" would represent a failure to collaborate in necessary global actions against terrorism. This scenario is more than improbable. The GDPR says at (4) finding "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right". The mankind progress means to share data what brings to share "sovereignty"."

The political economy of data science has a big role. The political economy of the IoT has to settle the basis of the inter-connectedness between data and physical hardware and their relationship with different elements, such as laws, business practices, standards, capital, territories or markets, sectors, production processes, and so forth. This is probably a work of more than one Government or country. Probably those who make, deploy, operate and own the network infrastructure and devices will be determined by the control of data and data flows. The USA has developed amazing technology because of the American model of information privacy. But the strength of EU law model can slow this progress.[viii] Europeans have enjoyed the benefits of American technologies, but human rights have to be respected too by the American products and services.

REASONABLE EXPECTATIONS FROM USA/UE

European laws permit a blockage of international transfers of personal information. At the transnational level, the EU has created legal instruments that permit the blockage of data transfers to countries with inadequate protections. The USA is one of the countries with inadequate protection. The decision to permit a specific transfer of personal information to the USA requires Europeans to evaluate the nature and the extent of data protection law in the USA. A narrow evaluation is required: the specific context of the planned transfer, the nature of the concerned data, and the specific legal protections in the USA for these data. But in Europe the individual right to personal data protection is connected to the legal system of data protection by inalienability of principles and rights. The individual cannot trade or surrender these rights and principles because they are an essential part of the democratic system:[ix] Principles in the Articles 5 (also 6 and 7); rights in the articles from 12 to 22, and article 51 established a "Supervisory Authority" for a strong protection of these rights.

This key point of the EU law in addition to the PII concept makes the understanding between the governments almost "impossible". However, the GDPR provides some fundamentals to create a new framework based on public interest, legitimate interest or national security:

(45) "Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation" (47) "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, into provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example"(50) "The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State."

The "legitimate interest of a controller" (finding number 47) as ground for data processing is supported by arts. 6.1.f; 13.1.d: 14.2.b. GPDR.

Art. 6.1.f: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

This ground can be completed by art. 23.1.e "other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;"

Based on these grounds, the Authorities can find a legal support to deal with the individual rights (especially "consent" and "purpose" of processing) in a more realistic and pragmatic way in a digital global world. Moreover, following the traditional American model, it is possible to break down the regulation taking into account different sectors and business. Governments can create legitimate legal bases to permit, for some business, a broad interpretation of "consent" or "purpose" in a way that the consent and purpose can be extended for specific contexts and purposes pursuing an specific interest or goal (which can transversal through companies and territories). And following the different specific requirements of every sector, companies devoted to freedom of information and expression and social networks[x] can be beneficiates by Chapter IX. Art. 85.1.:

"Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them."

And in article 89 is where "public interest" meets the broad spectrum of derogations, exceptions and exemptions.

Art.89: "Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processingwhich does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards

referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of those purposes.3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of those purposes.4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs."

Finally, because the GPDP does not apply to terrorism matters, USA/EU can agree on international law pertaining to surveillance, making clear the rules and guarantees binding for both sides (EU in USA and USA in EU), avoiding mass surveillance without knowledge. Obviously, it is time to share data sovereignty.

CONCLUSION

- Political decisions between the EU and USA are necessary before anything in order to find a new and temporary agreement because of the seemingly "irreconcilable" positions.
- To refine the concept of "personal data protection" in a realistic way taking into account the state-of-the-art technology.
- Global business, Internet of Things, Artificial Intelligence and global action against terrorism demand the sharing of data sovereignty.
- Public interest, legitimate interest, restrictions, exceptions, exemptions and derogations, could provide a legal bases based on the GDPR for a framework, where it is possible to agree to some flexible interpretation of rights and obligations in a digital context, respecting their essence and inalienability in a democratic system.
- Because "terrorism" is not falling in the material scope of GDPR, international law between the USA and the EU can determine "the red lines" in personal data to avoid illegal "mass surveillance".

REFERENCES

[i] Daniel J. Solove & Paul M. Schwartz, *Privacy Law Fundamentals* 2017. IAPP Publication, N.H, U.S, 2017, p.p. 253

[ii] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Abril 2016 on the Protection of Natural Persons with regard to the Processing of

Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

[iii] European Court of Justice (CJEU) Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner and other*. 2015. E.C.R. (Sept.23, 2015)

-About Snowden case, see: EUROPEAN PARLIAMENT REPORT 2009-2014 COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS 2013/2188 (INI) 23.12.2013. Report on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizen's fundamental rights and on transatlantic cooperation in Justice and Home Affairs.

[iv] General Data Protection Regulation (GDPR): article 4.1 (definitions).

[v] Mulligan Deirdre K. Mulligan, Colin Koopman, Nick Doty, "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy", Floridi L, Taddeo M (editors). *The Ethical Impact of Data Science. Phil. Trans. R. Soc. A;* 2016 374 (issue 2083)

[vi] Hellen Nissenbaun and Solon Barocas, "Big Data's End Run around Anonymity and Consent" (chapter 2) in *Privacy, Big Data, and the Public Good: Frameworks for Engagement* . Cambridge University Press, N.Y, 2014, p.p. 50

[vii] Steven Weber and Richmond Y. Wong, "The new world of data: Four provocations on the Internet of Things". *First Monday*, Volume 22, Number 2 - 6 February 2017 http://firstmonday.org/ojs/index.php/fm/article/view/6936/5859 doi: http://dx.doi.org/10.5210/fm.v22i2.6936.

[viii] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on The Ground. Driving Corporate Behavior in the United States and Europe*. MIT Press, MA, 2015

[ix] Paul Schwartz, "Consent and Contract under EU Data Protection Law", *6th Annual BCLT Privacy Law Forum*. Silicon Valley. Berkeley Center for Law & Technology. March 24, 2017

[x] Rosa María García Sanz, *Digital Journalism. Rethinking Communication Law to Support Democracy and Viable Business Models*. Academica Press, LLC. Palo Alto, California, 2017, p.p. 141 y ss