CHAPTER 3. EU vs. US: the two major schools of thought regarding internet and privacy regulation and why they took divergent paths. Can this distance be bridged in the context of a regulatory framework for the cloud?

a. Introduction – scope of the chapter

It is commonly accepted and can be also verified through figures[130] that the EU and the US have been the two most important players when it comes to the issue of internet and privacy regulation[131]. The EU has managed to influence with its legislation on the fields tens of other national or regional jurisdictions worldwide, which have developed their privacy and internet laws very much following the essence and cornerstone elements of European legislation[132]. On the other hand, the USA, despite not having been equally successful in 'exporting' their legal approach regarding the above issues, have clearly managed to maintain a gravitas in the field due to their enormous share in the overall market size of the internet, both from the perspective of users and from that of service providers[133]. As it is known, these two jurisdictions have over the course of the years followed distinct paths as to how issues related to the development of applications of information technologies were regulated[134]. The distance between them was never totally bridged and it exists, as far as the issue of cloud computing is concerned, as well. However, given that the genuinely borderless nature of cloud technologies contradicts the fragmented regulatory landscape caused by divergent jurisdictional tendencies, in the context of an

130 Graham Greenleaf ed., Global Data Privacy Laws: 89 Countries, and Accelerating. Special Supplement, Issue 115 (2012.)

131 *Id.*

132 Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, 2 International Data Privacy Law 68–92 (2012.)

133 Graham Greenleaf, Major Changes in Asia Pacific Data Privacy Laws: 2011 Survey (2012.)

134 For more see Chapter 4.

analysis that seeks to bring together potential points of convergence on the matter between EU and US law, we must agree on a minimum common understanding that will permit not necessarily the convergence of different jurisdictions but most importantly the effective interaction between them. Over the course of this chapter, the different standpoints at which European and American laws about the internet and its subsequent phenomena have been traditionally standing, are summarized and presented. Then, the ground is set for ways in which these two schools of thought (and the numerous others that have been evolving under the influence thereof[135]) could approach each other and govern in a more pragmatic manner a state-of-the-art IT phenomenon, such as cloud computing.

b. How extensive is the influence of European data privacy standards outside Europe? Is it EU law that has been so influencing or is it more the entire European legal thinking?

One of the generally admitted facts about data privacy and regulation thereof worldwide is that a great deal of countries across continents have developed their respective laws by following the patterns and legal notions originally conceived in Europe[136]. However, despite the fact that popular belief usually attributes this wave effect to EU legislation, in reality it is the overall European legal tradition that has succeeded so much in shaping data privacy legislative standards on a global scale[137]. The two major areas and jurisdictions that have been exempt from the influence of the European school of thought in the area of data privacy, are the USA and China. The fact that these two countries have largely maintained their independent path in regulating data privacy related issues along with the economic and political power they both carry requires special consideration in any assessment of global data privacy developments[138]. Neverthe-

135 Graham Greenleaf ed. (note 130).

136 For more see Chapter 4.

137 L. A. Bygrave, *Privacy protection in a global context–a comparative overview*, 47 Scandinavian Studies in Law 319–348 (2004.)

138 Graham Greenleaf, *Global Data Privacy Laws: Forty Years of Acceleration*. *UNSW Law Research Paper No. 2011-36* Privacy Laws and Business International Report 11–17 (2011) (Significant as China's role may be in the state of affairs regarding privacy and internet regulation on a global scale, it falls outside the scope of this study to assess the Chinese effect on the future of privacy and cloud com-

less, the increasing pressure for change these two jurisdictions face, especially in recent years, must also be pointed out.

In the USA, there are many privacy laws with relevantly effective enforcement, but no comprehensive privacy law in the private sector[139]. What is more, despite the fact that the revelations of latest years have increased pubic outcries for more comprehensive protection of privacy, there is not much real prospect for a comprehensive legislative package on the matter, despite periodic calls for one from major companies or draft Bills introduced into Congress. It is not of course the case that the USA does not have any standards for (private sector) data privacy; the main problem is rather that they must be inferred from many scattered pieces of legislation, while, in various sectors, there is utter absence of any significant legislation[140]. There are also some State constitutional protections along with common law structures[141]. All of the above lead as a fact to a situation that often makes scholars claim that the US approach is incoherent, sectoral-based, and with legislative protections that are largely reactive, driven by outrage and at particularly narrow practices[142].

On the other hand, since everyone admits that 'European standards' for data privacy have been influential on a global scale, we need to devise ways in which we could measure that. It is also essential to check whether the causes of influence can be traced, apart from its effects. With a very small number of exceptions (Israel, public sector laws in some OECD countries, New Zealand) data protection laws outside Europe were adopted in the aftermath of the 1995 Directive[143] (or at least in the aftermath of

---

puting regulation. For structural, as well as practical barriers, e.g. the language barrier, this project focuses on the European and US jurisdictions alone.)

139 Elisa Bertino, Ravi Sandhu, Lujo Bauer & Jaehong Park eds., the third ACM conference.

140 Chris Hoofnagle, COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS. B.1 – UNITED STATES OF AMERICA, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf (2 May 2016.)

141 *Id.*

142 Graham Greenleaf (note 132).

143 Directive 95/46/EC 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, 24 October 1995, (OJ) L 281, 23/11/1995 P. 0031 – 0050.

the introduction of its draft form in the early 90s)[144]; consequently, they were open to influences from it at their inception. In certain cases, even revised laws (for instance, those of Taiwan, South Korea and New Zealand) have incorporated new elements in their body influenced by the EU Directive[145].

If one would like to present a comprehensive picture about how laws outside Europe have been influenced by the European legal thinking about data privacy regulation, one would need to pinpoint two big pools of influences: (i) those which can be attributed to both the EU Directive and the OECD Guidelines[146]; and (ii) those which are found in the Directive but are not required by the OECD Guidelines[147]. In literature, it has prevailed that the first are called influences with 'global' and the second influences with 'European' origins[148]. All of them put together, they prove that it is not EU law that has had such a profound influence on global standards for data privacy regulation but, in fact, European legal thinking in its entirety.

Those ten plus ten influences offer a comprehensive picture about the most common elements that define data privacy in the online world currently across jurisdictions worldwide. In particular, the ten influences with 'global' origins, i.e. notions that are common to all three major international instruments governing online (data) privacy that have started developing in Europe[149] plus the APEC Privacy Framework[150] of 1998 (which was lastly revised in 2004) are[151]:

---

144 *Id.*

145 *Id.*

146 The comprehensive set of OECD guidelines on privacy and transborder flows of personal data is available here: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (lastly accessed 02/23/2017.)

147 L. A. Bygrave (note 137).

148 Graham Greenleaf (note 132).

149 These instruments are: the EU Data Privacy Directive of 1995, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 (ETS 108).

150 The APEC Privacy Framework (1998) is available here: http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf (last accessed on 09/11/2017.)

151 Graham Greenleaf (note 132).

- **Collection**, which has to be limited, lawful and conducted by fair means; with consent or knowledge of the data subject [OECD 7; CoE 5(c), (d)]
- **Data quality**, which requires that any data collected need to be relevant, accurate and up-to-date [OECD 8; CoE 5(a)]
- **Purpose specification** at time of collection [OECD 9; CoE 5)]
- **Notice of purpose and rights at time of collection**, which have to be communicated to all data subjects [OECD ambiguous; APEC stronger; CoE not explicit but implied]
- **Uses of collected data have to be limited** (including disclosures) to specified or compatible purposes [OECD 10; CoE 5(b)]
- **Security of data has to be continuously maintained** through reasonable safeguards (OECD 11; CoE 7)
- Personal data and the **practices applied** to them **need to be open and clearly stipulated** at all times [OECD 12; CoE 8(a)]
- **Access**: data subjects need to have individual right of access to their data at all times [OECD 13; CoE 8(b)]
- **Correction**: the data subject needs to have the individual right of correcting the data relevant them [OECD 13; CoE 8(c), (d)]
- **Accountable**: data controllers are to be held accountable for implementation of previous nine points (OECD 14; CoE 8)

Then, there are these ten influences with 'European' origins that may or may not be found in national privacy laws[152]:

- Requirement of an independent Data Protection Authority as the key actor of an enforcement regime (EU Directive, and Additional Protocol to Convention 108)
- Requirement of recourse to courts to enforce data privacy rights (EU Directive, Convention 108 and more explicitly the Additional Protocol to Convention 108)
- Requirement of restrictions on personal data exports to countries that do not meet sufficient standards of privacy protection (defined as 'adequate') (EU Directive, and Additional Protocol to Convention 108)
- Collection of data must at each time be the minimum necessary for the purpose it is executed, not simply 'limited' to this purpose (both EU Directive and Convention 108)

152 *Id.*

- A general requirement of 'fair and lawful processing' (not just collection) (both EU Directive and Convention 108)
- Requirements to notify, and sometimes to provide 'prior checking', of particular types of processing systems (EU Directive)
- Destruction or anonymization of personal data after a certain period (both EU Directive and Convention 108);
- Additional layers of protections for particular categories of sensitive data (both EU Directive and Convention 108)
- Limitations on automated decision-making, along with a right to know the logic of any automated data processing arrangement (EU Directive)
- Requirement to provide 'opt-out' of any direct marketing use of personal data (EU Directive).

c. What is the main difference from Europe in USA's arrangement of their regulatory framework for privacy and the internet?

There are several reasons which serve to explain why the United States have not been anywhere near as successful as Europe in exporting their legal culture on privacy and the Internet to third jurisdictions. However, before moving into seeking the answers to this questions, one observation is essential: There is a fundamental difference in the way the issues of data privacy and internet regulation have been built so far compared to Europe and the European Union, in particular[153]. In fact, the United States continues to lack an omnibus law that would cover, in a comprehensive manner, all these issues in the private sector. At the same time, it has, at best, only a relatively limited omnibus law for part of the public sector[154]. This is in stark contrast to what happens in Europe, where new countries that have joined the EU, have quickly adapted their regulation of information privacy with omnibus laws. Then, they have supplemented these statutes with sectoral ones, wherever further details in regulation where necessary. According to many scholars, this continuing difference between Europe and America can best be explained by the following two factors[155]:

153 Elisa Bertino, Ravi Sandhu, Lujo Bauer & Jaehong Park eds. (note 139).
154 Paul M. Schwartz & Daniel J. Solove (note 16).
155 Paul Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harvard Law Review 1966–2009 (2013.)

– initial regulatory choices which were then solidified as a pattern by path dependency in each jurisdiction, and
– the usefulness of omnibus laws in multinational systems, such as the European Union, that wish to harmonize their regulations compared to the tendency of federal systems, like the USA, to prefer regulatory arrangements and more multi-layered regulatory structures.

There has been a lot of discussion as to whether a federal US law on privacy would be a good or a necessary thing. It is certain that the consequences from a unifying federal legislation would be both positive and negative. On the one hand, an omnibus law would overcome the inability of sectoral laws to respond adequately to telecommunications convergence, which is one of the most prevalent processes on the Internet[156]. In addition, omnibus laws tend to level the regulatory playing field while sectoral laws can place unequal burdens on industries in closely related areas[157]. Last but not least, an omnibus law is considered by many that it could help convince the EU of the adequacy of US privacy laws, thereby assisting in smoothing data flows between the two markets[158]. However, there is a good deal of people who tend to criticize an eventual movement of the US towards the adoption of omnibus legislation on privacy. They cite as the most important reasons for this criticism the costs that an extra layer of regulation would give rise to, and the risk of an omnibus law's obsolescence due to latency in the pace of its reform cycles[159].

d. The 'privacy collision' between Europe and the USA: a brief historical overview

Having pointed out how the USA, as a legal culture and jurisdiction have traditionally decided to deal with privacy in a diffusible, non-omnibus manner, it is worth briefly examining how Europe has moved through time in dealing with the same issues. At the end of this historical flashback, one will have already discerned some of the causes that made these two impor-

156 Paul M. Schwartz & Daniel J. Solove (note 16).
157 Paul M. Schwartz, *Preemption and Privacy*. UC Berkeley Public Law Research Paper, 118 Yale Law Journal 904-947 (2009.)
158 Paul Schwartz (note 155).
159 *Id.*

tant players in the privacy and internet regulation field follow so divergent paths.

On a European, as well as on a global level, it was the Hessian Parliament that enacted the world's first comprehensive information privacy statute in Wiesbaden, Germany, in 1970[160]. This piece of law was followed by similar ones of other German states[161], and in 1977 a Federal German law on privacy was adopted[162]. Other European countries closely followed suit in 1970s when Sweden (1973)[163], Austria (1978)[164], Denmark (1978)[165], France (1978)[166], and Norway (1978)[167] all enacted data protection statutes.

Europe has been also the stage for some of the most important supranational privacy agreements that were adopted even before the EU Data Protection Directive of 1995. The two most important, as it has already been demonstrated[168], are the Privacy Guidelines of the Organization for Economic Cooperation and Development (OECD) and the Convention on Privacy of the Council of Europe. The OECD principles, despite being non-binding, have had a great influence on numerous national laws.

Simitis, one of the academic forerunners in the field of data protection in Europe, summarizes the prevailing view about privacy in EU law already since its early days, as follows: "Data protection does not stop at national borders. Transfers of information must be bound to conditions that attempt in a targeted fashion to protect the affected parties."[169]

The impact of the Data Privacy Directive had been significant. Apart from shaping the form of numerous laws, inside and outside the EU, it contributed to the evolution and concretization of the well-known substantive EU model of data protection, which has been so highly influential. What is more, given the expressive preference for omnibus privacy laws,

---

160 Peter Gola, Christoph Klug, Rudolf Schomerus & Barbara Körffer, Bundesdatenschutzgesetz. Kommentar (2010.)
161 *Id.*
162 *Id.*
163 Nordic Council of Ministers, Information Security in Nordic Countries (1993.)
164 P. E. Agre & M. Rotenberg, Technology and Privacy: The New Landscape (1998.)
165 Nordic Council of Ministers (note 163).
166 P. E. Agre & M. Rotenberg (note 164).
167 Nordic Council of Ministers (note 163).
168 See also Chapter 4.1.
169 Ulrich Dammann & Spiros Simitis, Bundesdatenschutzgesetz (2014.)

European legal thinking contributed towards the establishment of regulatory standards with a broad scope in contrary to the limited protection guaranteed by sectoral laws.

These developments led to today's status quo with reference to privacy regulation in the US and Europe. Following the sectoral instead of the omnibus legislative route, the United States have different statutes on privacy for the public and private sectors. Within the private sector, they concentrate on the data holder and, in some instances, on the type of data[170]. In certain privacy statutes, there is an even deeper distinction related to the form in which the data is held, or the content of the information[171]. This approach has been thought by scholars to generally give a freer rein to data processors to try new kinds of processing[172]. This has been regarded as a boost to innovation as, particularly enterprises in new business areas, are largely free of regulation under a sectoral regime and thereby able to test innovative new practices; on the other hand, there is the opposite perspective which sees this greater freedom as fertile ground for new ways to violate privacy[173]. Another effect of this approach is the tendency that has been repetitively witnessed in the USA to place heavier data privacy restrictions on established enterprises than on new companies[174].

The two starkly different approaches have met equally diversifying critique from scholarly opinion. For instance, on the one end of the stick we find Joel Reidenberg, who, in a bold move already in 2000, took the view that between the US and the European approach on privacy there is a profound dichotomy. In particular, Reidenberg found that "US information privacy regulation was based on liberal norms and market forces, while the EU's information privacy regulations were based on "social-protection norms," where "data privacy is a political imperative anchored in fundamental human rights protection."[175]

A more positive take was adopted by scholars such as Anne-Marie Slaughter whose opinions are demonstrative of the scholarly thought that

---

170 Paul Schwartz (note 155).
171 *Id.*
172 *Id.*
173 Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex. L. Rev. 553–593 (1997.)
174 Reidenberg, J. R., Schwartz, P. M., Data Protection Law and On-line Services: Regulatory Responses.
175 Joel Reidenberg, *Yahoo and Democracy on the Internet* Jurimetrics 261 (2001.)

took a more insightful perspective on global privacy policymaking. According to Slaughter, "states now relate to each other through their parts and not their whole. States are disaggregated, that is, they interact not only through their foreign offices and state departments, but also through a variety of regulatory, judicial, and legislative channels"[176].

Extensive analysis of how the current EU Data Protection Regulation works are done in other parts of this study[177]. In terms of the evolutionary perspective of EU's data protection policymaking and the need for it to become more accountable and transparent the most promising element is Article 45[178] of the Regulation, which calls for collaboration in data protection on a global basis. For the time being, this is only a wish and encouragement for the future. However, a regulatory field such as the one of cloud computing would be an ideal one for putting this call into practice.

The evolutionary process of data protection laws in Europe and the USA and the point where we are right now, in terms of available technologies, IT applications which have already been or are about to be commercialized and, in particular, the appearance of cloud computing, big data, internet of things and artificial intelligence, not as small sectors of IT activity but as entire industries that have the potential to substitute or, at least, offer all-inclusive alternatives to practically all kinds of data processing and knowledge generation we used to do offline so far, call for much more proactive and generic policymaking and regulatory rules in the future. Both Europe and the US have to work towards laws that will not simply concentrate on a limited set of instances made possible through IT technologies or the cloud but towards legislation that will stand above individual occurrences and will bring the big picture in focus. At the same time, apart from promoting a more generic over a case-based approach, future IT laws need to set the foundations for a regulatory regime that will be able to work independently without the constant need for interventions from executive supervisory bodies such the Data Protection Authorities, in Europe, or the National Security Agency, in the USA. In other words, just as it has been done in other more conventional sectors of regulation, cloud computing and IT laws in general should be constructed in such a manner that they empower the actors in the very system that they regulate to make sure the system will work in a trustworthy manner. Proactivity instead of

176 Anne-Marie Slaughter, A New World Order (2009.)
177 For more see Chapter 4.
178 Art. 45, Regulation (EU) 2016/679 (GDPR) (note 25.)

interventionism is the answer to a sound legislative future for the cloud and this is what regulators need to try to achieve both in Europe and in the USA, even if they have to depart, of course, from the different points where their diversified legal traditions have led them today.

Homogeneity is not sine qua non for such a way forward. In Europe, privacy and data protection are heralded as fundamental rights that deserve erga omnes protection. Conversely, in the United States, the Constitution contains no express right to privacy. Instead, the American conception of privacy is practically synonymous to the 'right to be left alone' – a provision whose constitutional basis can be traced in the Fourth and Fifth Amendments of the Bill of Rights. As it has been put, in the core of the American version of the right to privacy still exists to a great extent 'the form that this took in the eighteenth century: it is the right to freedom from intrusions by the state, especially in one's own home'[179]. In essence, contrary to the path followed in Europe, privacy in the U.S. (as a constitutional right) has materialized as one exclusively assertable against the State[180]. This 'public nature' of the right to privacy still remains prevalent today, even though certain subsequent statutory laws have endorsed a legal right to privacy enforceable also in private affairs on the basis of a 'sectoral approach'[181].

Despite these profoundly differing courses, it is definitely possible and, at the same time, desirable for both EU and US law to move towards a more pragmatic direction with reference to laws for the cloud. An element that would certainly bolster this necessity and would invigorate a regime of governance[182] instead of one of continuous state inspection is self-regulation[183]. This would imply a certain degree of independence from state regulation, as market players would be responsible for regulating themselves by following common rules and self-enforcing them[184]. The consequences, in case of failing to abide by this legal obligation for self-regu-

179 K. S. Ziegler, Human Rights and Private Law: Privacy as Autonomy (2007.)
180 Paul Schwartz (note 155).
181 *Id.*
182 For more see Chapter 5.
183 National Telecommunications & Information Administration (NTIA), PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, available at: https://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age (4 May 2016.)
184 D. Tambini, D. Leonardi & C. T. Marsden, Codifying Cyberspace: Communications Self-regulation in the Age of Internet Convergence (2008.)

lation, would come at a stage prior to the occurrence of any detrimental incidents for the data hosted on the cloud or the subjects of that data. They will in fact be the repercussions of failing to prove that, as an actor of the cloud environment, one lives up to the duties expected from them, not as a result of allowing a network failure to cause damage to the data or the subjects thereof. In other words, responsibility will be asserted on a proactive instead of a punitive basis. In the actual business of cloud computing, self-regulation can be made more attractive as an approach if it is promoted as a means to increase professional reputation and preserve ethical standards[185]. Practically speaking, self-regulation can be achieved by promoting certain practices (interoperability, privacy-compliant services, etc.), from the one hand, and banning or heavily discouraging others kinds of activities that might negatively affect users (user-profiling, targeted advertising, arbitrary censorship, etc.) on the other[186].

Nevertheless, this is not to imply at all that the State would have no role to play in a future cloud computing regulatory regime. In fact, the very way in which cloud services exist today, along with the dominance of the cloud market by a few large corporations, mean that private regulation amongst market players alone is unlikely to lead to satisfactory results. The state will continue to play a decisive role in the future cloud governance structure as the extra-network actor that will be tasked with intervening in order to push self-regulation towards the right direction[187]. Indeed, despite the fact that self-regulation concerns market players, to the extent that they operate within the boundaries of sovereign states and their respective jurisdictions, they are nonetheless subject to national rules[188]. As a result, state regulation can serve as the necessary backbone and provide the incentives for cloud providers to regulate themselves in a manner that effectively responds to users' demands and expectations[189].

In addition, self-regulation should not be limited to the realm of market players; in response to the sectoral diversification the cloud applications and uses demonstrate, it could be implemented amongst specific communities of users belonging to specific sectors who are eager to autonomous-

185 Andrew Charlesworth, *Clash of the Data Titans? US and EU Data Privacy Regulation*, 6 European Public Law 253–274 (2000.)
186 *Id.*
187 D. Tambini, D. Leonardi & C. T. Marsden (note 184).
188 National Telecommunications & Information Administration (NTIA) (note 183).
189 Andrew Charlesworth (note 185).

ly establish the rules they will have to abide to, rather than observing rules dictated by third party cloud operators[190]. This typology of self-regulation stands out from the self-regulation of cloud operators as it does not primary rely on pre-fabricated contracts or codes of conduct, but rather on technical arrangements (hardware or software) developed by users to tackle what has not been properly addressed by cloud operators[191]. In conclusion, self-regulation rules addressed to users (coming from specific sectors) will act as a form of self-discipline with private origins effected through bottom-up technical regulation[192].

e. Personal data privacy in Europe and the US: a pragmatic and an articulate approach

The evolution of the European and the American doctrine on privacy has led to the current legal approaches of the two jurisdictions on the issue of personal data privacy. Europe has nourished through the years a more pragmatic approach. In particular, Community lawmakers had to bridge the gap between the 'ideal' of the Single Market for unrestricted and unregulated movement of all personal data within the EU Members' area and the requirements of the Council of Europe's (CoE) Convention on the Automated Processing of Personal Data[193], to which all EU Member States are signatories[194]. The latter stipulates that any information about individuals which is to be automatically processed has to be handled in such a manner that the privacy rights of the subjects of this information are protected[195]. At the same time, CoE's Convention encouraged the establishment of a common international standard of protection for individuals[196], with the aspiration that the free flow of information across international boundaries could proceed without interruptions. In the end, EU law had to

190 D. Tambini, D. Leonardi & C. T. Marsden (note 184).
191 Andrew Charlesworth (note 185).
192 *Id.* .
193 Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (note 148.)
194 C. J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (1992.)
195 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (note 148.)
196 Id.

strike a balance between various country interpretations of this goals: for a number of them, such as Germany, France and the Nordic countries, these issues had been understood as having a significant human rights element. For others, such as the UK, the primary concern turned to be making sure that the minimum standards of protection required by the Convention were ensured so that international trade may not be disrupted[197]. These diversified tendencies were attempted to be abridged by means of the Data Privacy Directive which elevated the concept of personal data privacy into a concrete and enforceable privacy right[198]. As it was stated in Article 1 of the Directive: 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'[199] Finally, the currently applicable General Data Protection Regulation is an effort to further concretize the nature of privacy of personal data as a fundamental right mainly by increasing the means or possibilities for individuals to verify or keep under control the circulation of their data[200].

The United States have concretized through the years a more complex approach on the issue of data privacy[201]. Despite the lack of an explicit constitutional provision for a right to privacy, the concept of privacy in the sense of 'the right to be left alone' has traditionally been entertained in principle by the US legal system, despite having been only rarely genuinely supported in practice when it comes to informational privacy.

Nevertheless, the types of privacy issues that federal and state legislators and courts have dealt with so far in the US tend to revolve around physical or decisional privacy[202]. What is more, these US constitutional privacy rights are always exercised against either federal, or state, government, i.e. they prevent the government from degrading individual citizens' rights; they do not require them to protect these rights against third parties. This is by no means to imply that the USA lack personal data privacy

197 Andrew Charlesworth (note 185).
198 For more see Chapter 4.
199 Directive 95/46/EC (DPD) (note 143.)
200 EU General Data Protection Regulation (note 25.)
201 Primavera De Filippi & Internet Policy Review, Foreign clouds in the European sky: how US laws affect the privacy of Europeans (2013.)
202 S. Scoglio, Transforming Privacy: A Transpersonal Philosophy of Rights (1998.)

laws. What the USA lack, however, is a coherent personal data privacy framework and any meaningful enforcement mechanism[203].

In summary, it can be argued that the key differences between the EU and US approaches to privacy are more in the mechanics of achieving data privacy than in the concept itself. The essential difference between them lies with the fact that EU laws provide for a legislatively backed data privacy regime, applicable to both public and private sector, overseen by regulatory authorities and with remedies to individuals whose data privacy rights have been breached. This renders the US strategic choice to leave privacy matters in the private sector untouched as the main obstacle towards a convergence of data privacy laws between the EU and the USA[204].

However, for the comparative presentation of the two approaches to be complete, it is meaningful to also present the arguments against the US adopting a similar regime, which can be summarized to the following points[205]:

– the USA should not comply with the extraterritorial application of another jurisdiction's laws[206];
– trade in personal data in the USA is so advanced that it is too late to provide a data privacy regime[207];
– a centralized government privacy regulator is not trustworthy; at the same time, centralization of data and knowledge about data protection is a graver threat to personal privacy than commercial activity involving data[208];
– the cost of compliance would outweigh the social benefit[209];
– such a radical change of course would hamper information-related businesses and would slow their expansion into global markets[210];

---

203 Paul Schwartz (note 155).
204 *Id.*
205 Chris Hoofnagle (note 140).
206 Peter P. Swire & Robert E. Litan, None of your business. World data flows, electronic commerce, and the European privacy directive (1998.)
207 Andrew Charlesworth (note 185).
208 Paul T. Jaeger, Jimmy Lin, Justin M. Grimes & Shannon N. Simmons, *Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing*, 14 First Monday (2009.)
209 Andrew Charlesworth (note 185).
210 Paul T. Jaeger, Jimmy Lin, Justin M. Grimes & Shannon N. Simmons (note 208).

- the way the US Constitution is modeled may prevent the federal government from engaging in European-style regulation of personal data use[211]; and
- deliberate self-regulation is a more effective approach than legal regulation.

f. Cyber challenges and state-of-the-art in Europe and the USA

Before concluding the analytical comparison between Europe and the USA regarding their legal traditions and treatment of online data privacy, the Internet and related phenomena, it is essential to go over the latest and current developments about these issues in the two jurisdictions. In this way, the state-of-the-art picture in the two jurisdictions will lead to evidence about the course future cloud computing laws will need to follow so that an overall efficient regulatory regime for the cloud is achieved among different jurisdictions on a worldwide scale.

i. EU's approach towards cyber challenges

The EU has recently taken a decisive step by introducing the General Data Protection Regulation into force[212]. However, and despite the undoubted novelties that this new piece of legislation introduces in the field of data protection, it largely focuses on just one aspect of the uses of technologies like cloud computing, leaving aside the cloud as a broader regulatory phenomenon per se. Additionally, the GDPR continues on Europe's tradition on regulating privacy from the perspective of a human right that needs to be defended against malpractice. Nevertheless, few, if any, new elements are added that reflect on the true nature of cloud computing, that of a generic IT technology, which regulation-wise cannot be dealt with on a case by case basis but needs laws with a holistic approach. Even if the EU succeeds in creating an abuse-proof environment of cyber security within its borders (which is in itself a very ambitious and not necessarily realistic goal), it can by no means be totally immune to the threat of cyberattack. At the end of the day, when arguing about cyber issues, it is vital to keep

211 Paul Schwartz (note 155).
212 For more see Chapter 4.

in mind that the internet, as a borderless environment, guarantees no protection from outer coming threats. In today's digital environment, a cyber-attack on an EU target will more likely originate from outside the EU than from within.

It is high time for Europe to live up to its role as a global economic and political power and exert its political strength and outreach capacity to the international field as well. Cyber security has an enormous impact on the global economy and can affect the general public in many different ways as it has already been demonstrated. Securing the personal data of consumers and the general public should be of the utmost importance not only for regulators but also for the international private sector and state institutions. However, it is imperative that soon these goals are pursued not only on an ex-post basis but also on a proactive basis by switching their focus from correcting damage when it is done or by adding layers of control that may hinder damage to occur to ensuring that the cloud and cyber environments, in general, are properly built up and continuously run in a manner that upholds these values and effectively eliminates (or seriously limits) the chances of such unfortunate damage to happen.

What is more, although personal data security may be the major, or most common, kind of damage that may occur through cloud computing, it is crucial to understand that data protection is only an element within the broader challenge of "the misuse of technology"[213]. Besides, apart from the fundamental right aspect of data privacy, mishandling personal information can be much more than simply the means of very lucrative accumulation of wealth. The cloud, and the internet that is facilitated thanks to it, can be abused by terrorist organizations, organized crime groups, cyber warfare and espionage on the part of states. Moreover, a cloud based internet can also be manipulated (and, in fact, more effectively than the pre-cloud Web) for the proliferation of cryptocurrencies and the promotion of cyber underground economy. In a nutshell, Europe has done enough to develop a protective shield for the human rights put at risk for its subjects due to the expansive transposition of data-related processes from the offline to the online realm. On a long-term level, what the EU needs to focus on is not changing or substituting its existing data related legal tools but rather on complementing it with laws that will realistically regulate the en-

213 Francesca Bosco, Assessing Europe's cyber challenges, available at: http://policyreview.info/articles/news/assessing-europes-cyber-challenges/355 (4 July 2016.)

vironments where such data damage may occur[214]. The most prominent field of this kind nowadays is probably the cloud.

ii. The US approach towards cyber challenges

In the wake of 9/11 and the threats to national security the USA faced over the last 15 years, the country's legal landscape for the internet and online privacy was not left unaffected. In fact, these incidents led US lawmakers to pass bills that reflected the profound aftermath of those historic attacks -which were to a crucial degree made possible thanks to data or security breaches – both on the internal and on the external affairs of the USA. The two most crucial of these acts were:

– the U.S. PATRIOT Act[215] and,
– The U.S. Foreign Intelligence and Surveillance Act

The USA PATRIOT Act is only one aspect of the problematic landscape regarding privacy that currently exists in the USA. Most of the US safeguards for privacy that have been discussed so far are instantly invalidated when confronted with a much more intrusive (although, interestingly, much less debated) piece of U.S. legislation, the Foreign Intelligence and Surveillance Act (FISA)[216], which provides for special procedures for conducting physical searches and electronic surveillance of individuals allegedly involved in international espionage or terrorism against the United States of America[217].

The landscape that has been displayed above on both coasts of the Atlantic makes imperative the need for an international coordination for the future of IT laws, even those regulating data protection. While the European Data Protection Regulation introduced new safeguards aimed at fur-

---

214 *Id.*

215 United States of America: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act) [United States of America], Public Law 107-56, 107th Congress, 26 October 2001. For more see Chapter 7.

216 The Foreign Intelligence Surveillance Act of 1978 (FISA), Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36, is a United States federal law. It has been repeatedly amended since the 9/11 attacks.

217 Tridimas, T., & Gutierrez-Fons, J. A., *EU Law, International Law, and Economic Sanctions against Terrorism: The Judiciary in Distress?*, 32 Fordham International Law Journal 660–730 (2008). For more see Chapter 7.

ther reducing the risks of EU citizens' data being handed over to the US or other third countries' governments, concerns are expressed as to whether European authorities will properly address these issues out of fear of not decisively standing up against US authorities[218]. Others point one more danger out: the possibility that European intelligence services may try to circumvent EU law and benefit from the surveillance activities of the U.S. government that has a much wider margin of freedom as it has been demonstrated, in order to obtain information that could not be lawfully collected under European law[219].

As things stand right now, Europeans wishing to enjoy the maximum protection for their online presence, may only achieve that by storing their data exclusively on European cloud computing platforms operated by EU-based service providers. However, except for any setbacks that such a strategy could set on cloud adoption in the EU, it is a viable only for citizens living within the EU. It cannot for work for non-EU residents or EU citizens residing outside the EU, who may ultimately be subject to the laws of the country they live in. Yet, in a global and increasingly connected online world, the EU, as the most influential global legislator on privacy and internet issues, should lead the way and take actual care not only of the privacy of EU citizens but it should pave the path towards the establishment of a more comprehensive framework of international rules when it comes to privacy and data protection. More broadly, the EU needs to take actual steps towards an improved system of internet governance, with more sophisticated models of laws and/or standards which are properly adapted and constantly updated to the latest advancements in cloud computing[220].

g. Can cloud computing be a tipping point for regulating and thinking about privacy in the US or Europe?

Moving towards the concluding observations on how Europe's and USA's legal cultures have evolved through time in relation to the issue of online

---

218 L. Moerel, *Back to basics: when does EU data protection law apply?*, 1 International Data Privacy Law 92–110 (2011.)

219 *Id.*

220 Kristina Irion, *Government Cloud Computing and the Policies of Data Sovereignty*, 4 Policy and Internet 40–71 (2012.)

data privacy, it is time to examine whether up to this point the massive expansion of cloud computing has already initiated any profound processes of change in the two jurisdictions and the way they deal with these issues.

i. Privacy under the effect of the cloud in the US

In the US, the piece of law most relevant to the technological status quo effected by cloud computing is the Stored Communications Act[221]. The privacy protection that a user of cloud services will have the right to enjoy under the Act is currently dependent on the cloud provider's terms of service (ToS) agreement and privacy policy[222]. Actually, whenever the ToS agreement permits to the cloud provider to rely on customer's data in order to determine the contextual advertising it will channel towards him, that cloud service does not qualify as a remote computing service (RCS). Similarly, when the cloud provider in its ToS agreement reserves a general right to access customer's data without setting specific limits for that possibility, this cloud service is also unlikely to qualify as an RCS[223]. It is only when a cloud provider sets expressive limitations to its access to customer's data solely for the purposes of providing computer storage or processing functions that the customer benefits from the Act's RCS provisions, including the protection from compelled disclosure by the government and civil litigants[224].

It becomes evident that the margin for granting protection to a customer's data under the Act is much narrower than that of excluding the said data from protection. However, the consequences of being excluded from the Stored Communications Act privacy protections can be substantially significant for a cloud services user. Experience has shown that the US government have limited restrictions in assessing whether or not they

---

221 The Stored Communications Act (SCA) (note 31) is a US law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA).

222 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

223 *Id.*

224 *Id.*

have the ability to compel disclosure of a customer's data[225]. A user might try to fight back by revoking a Fourth Amendment privacy right, but such a defense has not prevailed in past cases involving email[226]. These facts suggest that US courts under the current status quo would be unlikely to extend privacy related constitutional protections into the realm of cloud computing. Simultaneously, the only effective limit to the ability to disclose a customer's data to a third party under US law is currently the contractual promises made in the cloud provider's ToS agreement and privacy policy. Unfortunately for users of cloud services, these protections are, as a rule, weak or nonexistent. As a result, cloud providers under the nowadays applicable US law have complete discretion in deciding whether to respond to requests for their customers' data or personal identifying information[227].

As more and more Americans move their personal content to the cloud, a respective upgrade in the privacy regime seems appropriate. There are, however, serious obstacles that would need to be tackled for this new concept of privacy to be made feasible.

ii. Judicial obstacles

Fourth Amendment jurisprudence indicates until today that courts are unlikely to uphold elevated privacy protections for cloud computing users. In the US, courts only rarely act as the initial forum for expanding privacy protections; when they do, it is typically through very reluctant extensions of the Fourth Amendment principles, under the pressing effect of societal or technological change[228]. However, as it has been already demonstrated[229], the Supreme Court has been formulating an ever-narrower view of the Fourth Amendment's provisions and the applicability of them. Lately, the Supreme Court has focused its Fourth Amendment handling on weigh-

---

225 Susan Freiwald & Patricia Bellia, *The Fourth Amendment Status of Stored E-mail: The Law Professors' Brief in Warshak v. United States* Journal Articles 559–588 (2007.)

226 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

227 *Id.*

228 Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Michigan Law Review 102–183 (2004.)

229 See Chapter 7.

ing the costs and benefits of decisions excluding evidence gathered in breach of the Fourth Amendment and on limiting the range of situations that merit Fourth Amendment protection. Overall, the way the Supreme Court has treated its Fourth Amendment jurisprudence allows for limited hope only as to the chances that it will drastically expand the extent of privacy protections for Internet users[230]. The main argument why it will still be too difficult for such a turn in jurisprudence to happen is that not only would such a shift change the dimensions of the Fourth Amendment's scope but it would also require reassessing core privacy principles, such as the third-party disclosure doctrine[231], that would have extensive repercussions as to how the US treats privacy beyond the digital world.

iii. Legislative obstacles

it is not up to a legal study like this to deal with factors external to the law making and judicial process that could impede (or enhance) evolution of legislature. Nevertheless, a few observations can and should be made as to the legislative and political landscape in the US in which the need for effective regulation of cloud computing has to mature. Although the US Congress has historically been favorable to the calls for enlargement of privacy protections, it is unlikely to lead the way towards expansion of the protective realm in the direction of online privacy[232]. This standstill could possibly be overcome with the right combination of catalysts like political momentum and societal demand. It is beyond the aims of this study to analyze what is the current balance of powers in the US Congress and

230 Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 Georgetown Law Journal 357–405 (2003.)

231 The third-party doctrine is a United States legal theory stipulating that people who voluntarily give information to third parties—such as banks, phone companies, internet service providers (ISPs) etc.—have "no reasonable expectation of privacy." A lack of privacy protection enables the United States government to obtain information from third parties without a legal warrant and without any other formality in compliance with the Fourth Amendment prohibition against search and seizure without probable cause and a judicial search warrant. Libertarians and liberals traditionally call this government activity unjustified spying and a violation of individual and privacy rights. For more, see Orin Kerr, *The Case for the Third-Party Doctrine*, 107 Michigan Law Review 561–601 (2009.)

232 Orin S. Kerr (note 228).

whether this is favorable for online privacy issues or not. However, even if there is societal demand for greater online privacy protections, a certain amount of time is needed before this is observed and realized by elected officials and judges[233]. Unfortunately, the typical age range of members of US Congress and the Judiciary makes it unlikely that they are as responsive as necessary to societal expectations such as those stemming from emerging technologies. Younger populace embrace cloud computing services very fast, but the average age of legislators – as well as that of Justices on the Supreme Court – exposes a noticeable generational gap between law subjects and law makers[234]. It is therefore up to advocates for enhanced online privacy as well as scholars and academia to bridge this gap and convey to legislature the technological state-of-the-art and its implications for individual privacy, which calls for the respective changes or additions in the regulatory status quo.

iv. Societal obstacles

One last obstacle towards US laws adopting a more advanced approach towards online privacy is the changing societal views toward the issue. In general, younger generations have much less concern about online privacy than older generations[235]. This differentiation can to a certain extent be explained by the different ways in which each generation uses the Internet. Older users generally engage into transactional encounters online, such as looking up information from websites, exchanging e-mail, or purchasing goods[236]. On the contrary, users from younger age groups embrace the internet's interconnectivity by engaging in social networking, sharing content, and adopting cloud services[237].

Another important element decisively shaping cloud users' privacy expectations is their growing expectation to receive 'free services' from cloud providers. In fact, especially younger users declare to be comfortable with cloud providers analyzing which websites they visit, what kind

233 Susan Freiwald & Patricia Bellia (note 225).
234 *Id.*
235 John G. Palfrey & Urs Gasser, Born digital. Understanding the first generation of digital natives (2010.)
236 Older Adults and Technology Use (2014.)
237 Susan Freiwald & Patricia Bellia (note 225).

of data they store online or other similar data that enable them to deliver targeted advertising[238]. From a market economics perspective, the frequency with which Internet users are willing to expose their online activities or exchange their personal data for free services and content suggests that they assign a low market value to their privacy[239].

h. Europe's combined approach towards the cloud and economic growth

Although the EU has not yet taken serious steps towards analyzing the specific challenges and characteristics of the cloud in order to regulate it, it has already realized its economic significance and the expansive effect it will have on many of the world's economies. This explosive global demand for cloud services, especially in emerging economies, has served as a cornerstone of the European cloud strategy[240]. The European Commission has explicitly addressed the paradox of a growing demand in cloud services as opposed to the slower progress of engineering science in Europe or the lack of a 'cloud-friendly' environment in Europe so that the continent can be at the forefront of global cloud developments. So far, the two main steps taken to amend this situation have been:

– negotiating free trade agreements that contain favorable conditions for EU-based cloud service providers

This method of 'positive conditionality' that the Commission implements in relation to cloud development is not new. It was also utilized by the US in the early 2000s with regard to the regulation of internet service providers (ISPs)[241]. Its reasoning is that third countries that wish to conclude free trade agreements with the European Union are requested to develop a regulatory framework for cloud-related matters that will be in line with Europe's respective regulatory framework so that EU-based cloud service providers can more easily lay foot on those markets.

---

238 William Jeremy Robison, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 Georgetown Law Journal 1195–1239 (2010.)

239 *Id.*

240 Osvaldo Saldias & Internet Policy Review, Cloud-friendly regulation: The EU's strategy towards emerging economies (2013); Reinhard Posch, *Neue Herausforderungen für eine Informations- und Datensicherungsstrategie*, 2014 Strategie und Sicherheit (2014.)

241 Digital Agenda in the Europe 2020 strategy (2012.)

– deliberations and close contact with key cloud stakeholders

The second pillar of the EU's cloud computing strategy is fostering an intra-European dialogue with key actors of the broader cloud ecosystem[242]. In order to tackle current problems and challenges of cloud computing within the European digital single market, the Commission is fostering several initiatives which aim to bring if in direct contact with key actors of the cloud sector, who through these channels will have the opportunity to express their concerns and propose their ideas for generating solutions to problems or tackling challenges. It remains to be seen, however, to what extent this input from market stakeholders is indeed taken into account in the future handling of the Cloud by the European authorities or not.

i. A close look on how the EU and the US currently handle sensitive consumer data on the cloud. It the current regime adequate and efficient enough?

Before wrapping up this all-inclusive comparison between Europe and the USA and how the two legal cultures currently deal with issues associated or generated out of cloud technologies, as well as how they deal with the cloud itself, one last aspect merits careful presentation: the handling consumer data receive in each of the two legal environments. As individual users are undoubtedly the most powerful driving force behind the cloud's geometric expansion, it is crucial to have a clear picture of how the data generated by this type of users are handled. Answering this question is easier from the EU perspective since the EU Data Protection Regulation contains in itself a precise definition of sensitive data when talking about 'special categories of data' as 'personal data revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions' of natural persons[243]. This definition of special categories of data is, of course, closely connected and affected by the European view that data protection is a fundamental human right. Some EU member states currently include in the term of sensitive data additional categories of personally identifiable data such as informa-

242 European Commission, Unleashing the Potential of Cloud Computing in Europe, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF (20 November 2014.)

243 For more see also Chapter 4.

tion about consumers' debts, financial standing, or the payment of welfare benefits[244]. However, this regime is bound to be homogenized once the General Data Protection Regulation enters into full force.

In contrast, there is no clear definition for sensitive data in the United States or one that could serve as an analogous point of reference to the 'special categories' of personal data found in EU legislation. This is reasonable, of course, if one takes into account that, in principle, there is no generally applicable data protection legislation in that legal order. However, a careful analysis of federal privacy legislation in the United States brings forward certain types of consumer data that are entitled to solid data protection[245]; as a result, one could use them as a counter reference to Europe's sensitive data. The most prominent data categories of this nature are:

– data collected by websites that refer to children under the age of thirteen,
– data collected by financial institutions about their customers,
– patient data collected by health care providers and
– data collected by credit reporting agencies about consumers' credit history.

Despite the FTC[246], as the competent agency, not having expressly defined sensitive data, from its practice it can be broadly inferred that the above categories of data are classified under US law as sensitive. At the same time, the FTC also recognizes that whether a particular piece of data is sensitive or not may also depend on certain subjective considerations. Yet, in any case, excluding data related to consumers' protected classifications under discrimination laws from the definition of sensitive data is not uncommon practice. On the contrary, it very well fits the prevalent U.S. view that information privacy law is primarily an instrument aimed at prevent-

---

244 Douwe Korff, EC Study on Implementation of Data Protection Directive 95/46/EC (2008.)

245 Nancy J. King & V. T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 Am Bus Law J 413–482 (2013.)

246 The Federal Trade Commission (FTC) is an independent agency of the United States government, founded in 1914 by virtue of the Federal Trade Commission Act. Its principal mission is the promotion of consumer protection and the elimination and prevention of anticompetitive business practices, such as coercive monopoly. In the field of IT, the FTC is mandated with several tasks that make it the US analogous of Europe's Data Protection Authorities.

ing economic harm[247]. This approach is, of course, a juxtaposition from the fundamental human rights approach adopted by EU law, under which consumers are protected from a visibly broader scope of privacy harms.

i. Regulating privacy and security of consumer sensitive data in the cloud; the US current status quo

At present, it could be argued that the cloud computing industry faces limited legal restrictions in the United States, as all activities related to the field are largely permissible or unregulated. This is both a blessing and a curse for the industry. On the one hand, the lack of comprehensive federal legislation that would set minimum requirements regarding the protection of consumers' privacy in the cloud leaves considerable freedom of activity to US cloud businesses[248].

At the same time, the federal laws that define the specific categories of sensitive consumer data that were previously presented, mandate for sensitive data under these four statutes a protection regime analogous to the data protection for sensitive personal data provided for consumers in the EU[249]. However, in the absence of such industry-specific legislation there may be no requirement for businesses offering or using cloud services to guarantee information privacy for consumers' personal data. This leads to the other extreme, where information as crucial as a consumer's name, residence address, e-mail address, mobile phone number, income level, marital status, sex, and race do not qualify as sensitive and, hence, do not receive adequate privacy protection. Of course, before concluding that information privacy management is a matter of unlimited discretion for U.S. cloud businesses, it is important to examine other sources of law that may serve as foundations for privacy and security rights for consumers such as state privacy tort laws and federal or state consumer protection laws[250].

Across several US states there are statutes that require companies to inform consumers in advance about security breaches that may expose consumers' personal data to identity theft or other wrongful uses, despite the

247 Wesley Gee, *Internet Tracking: Stalking or a Necessary Tool for Keeping the Internet Free*, 20 CommLaw Conspectus 223–252 (2011.)
248 Nancy J. King & V. T. Raja (note 245).
249 *Id.*
250 Susan Freiwald & Patricia Bellia (note 225).

lack of a federal data breach notification law[251]. Another source of protection for consumers' privacy rights are state tort laws which may enable consumers to recover their data through the civil litigation process from businesses that misuse them[252]. The applicability of tort law in the field of security for sensitive data is not yet settled; nevertheless, civil lawsuits are increasingly being brought by consumers as a means of redress for such claims[253].

To sum up, although at present there are only few U.S. laws that restrict the growth of cloud computing industry, and the regulatory framework for the cloud heavily relies on contractual agreements between CSPs and their clients or industry self-regulation, issues such as the uncertainty regarding the applicability of the USA Patriot Act and related federal statutes against global CSPs sets legal obstacles to unhindered cross-border provision of cloud service between the United States and the EU.

ii. Regulating privacy and security of consumer sensitive data in the cloud; the EU current status quo

In contrast to the current legal framework in the USA, European rules set high compliance obligations for companies active in the field of cloud computing requiring them to protect the privacy and security of consumers' sensitive data, including such data stored in public cloud facilities. EU laws establish two levels of consumer rights and compliance obligations for businesses dealing with personal data, a basic and a heightened one[254].

On the first level, the EU's Regulation grants to consumers (i.e. data subjects) a number of basic protections with regard to their personal data while it requires data controllers to abide by rules and restrictions with respect to their data processing operations. Additionally, consumers are entitled to receive notification about any data controller that expropriates their data as well as the purposes for which these are being collected or otherwise processed. On an advanced level, increased levels of data protection may also be required under the Regulation. For example, sensitive data

---

251 Nancy J. King & V. T. Raja (note 245).
252 *Id.*
253 *Id.*
254 *Id.*

that fall within the definition of 'special categories of data'[255] are entitled to increased data protection.

iii. The need for efficient protection of sensitive data also points towards regulatory reform in the cloud

All the above facts point out to the need for a fundamentally different regulatory approach for the cloud, both in Europe and the US. Cloud computing as a generic technology empowering today most variations of the IT economy and applications in the world calls for lawmakers to realize the true extent of the change the introduction of the cloud has signaled for all these areas of human activity[256]. Before drawing some general conclusions, we can now summarize the most important changes or innovations that sensitive data, in particular, call for in the way we will be regulating cloud computing:

– Working out a competent definition for sensitive data on the cloud

Right now, neither U.S. nor EU laws adequately define sensitive consumer data[257]. In the quest for an all-inclusive definition of sensitive data applicable in the global cloud computing industry, each jurisdiction could and should benefit from the other. Future laws governing the cloud should expand regulatory protection of sensitive data in such a way that both goals of encompassing the protection of human rights and avoiding economic and physical harms are effectively pursued. This pluralistic approach would clearly be in better alignment with information systems architecture for the cloud industry, which is largely defiant towards national borders, typically serves clients from every single country and jurisdiction and most often involves the processing and transfer of the personal data of users on a cross-country basis. A competent for current standards definition of sensitive consumer data should aim to prevent both discrimination on the basis of protected classifications as well as serious economic and

255 Andrew Charlesworth (note 185).

256 W. K. Hon, C. Millard & I. Walden, *Who is responsible for 'personal data' in cloud computing? --The cloud of unknowing, Part 2*, 2 International Data Privacy Law 3–18 (2012.)

257 Nancy J. King, V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 American Business Law Journal 413–482 (2013.)

physical harm[258]. A carefully planned step ahead for both US and EU laws for the cloud would adequately define sensitive consumer data to ensure efficient privacy and security for this kind of data on the cloud. Such a legislation and such a well-articulated definition would support administrative, industry as well as information technology best practices to establish themselves and be decisively mirrored in cloud service agreements thus guaranteeing better protection for customers, particularly since many cloud service agreements are effectively nonnegotiable due to the lack of bargaining power by users[259].

– In the US, moving towards comprehensive cloud computing laws

Even if existing US privacy laws are reformed to adequately clarify issues such as sensitive data and, thus, address the needs and concerns of users and providers of cloud services, they still lack an overall applicable federal information privacy regulation to govern the cloud. It is a historic opportunity for the US to take advantage of the generic nature of cloud computing and work out, for the first time in their legislative history, a robust, federal legislation for cloud computing that will also serve the broader need for a more federal approach on information security and privacy.

– In Europe, producing laws for the cloud that will keep on the continent's tradition of protecting privacy, as a human right, in ways more in line with the technological standards the cloud has established

Europe has an expressed intention of attracting more businesses to invest in cloud infrastructure on its soil, while existing cloud providers also put pressure on Europe to adopt a more business-friendly attitude towards cloud computing. In other words, both sides want the same thing and there has to be found the best way to pursue it. This could be achieved if Europe adopts a more receptive attitude towards technology solutions that could permit it to produce laws regulating the broader landscape the cloud has set. There are already, for instance, advancements in technology[260] that achieve anonymity of data in the cloud. These tools could be the implementing means of future cloud computing laws that would continue to serve Europe's long-held and much-cherished tradition of preserving pri-

---

258 J. Goldring, *Globalisation, National Sovereignty and the Harmonisation of Laws*, 3 Uniform Law Review – Revue de droit uniforme 435–451 (1998.)

259 Nancy J. King & V. T. Raja (note 245).

260 Response to the UK Ministry of Justice's Call for Evidence on the European Commission's Data Protection Proposals (2012.)

vacy as a fundamental right and, at the same time, make the EU area a much more favorable market for doing cloud business in.