FONDATION TELECOM

Think Tank
Futur Numérique

Cahier de prospective

The Futures of Privacy

Global Privacy Governance: A Comparison of Regulatory Models in the US and Europe, and the Emergence of Accountability as a Global Norm

Winston J. Maxwell

In the field of global privacy governance, we often hear of the tension between the European and US models. The clearest manifestation of this tension is the fact that the United States has not been found to provide "adequate" protection for personal data by the European Commission. Transfers of personal data to the United States are therefore tightly controlled.[1] Yet the United States and Europe have more in common than most people think. Both regimes are based on FIPPS, Fair Information Privacy Practices reflected in the 1980 OECD Guidelines. In spite of some philosophical differences, Europe and the United States can end up with similar practical solutions, such as for mobile apps. Importantly, both Europe and the United States are emphasizing co-regulation and "accountability" as regulatory models. APEC's Cross Border Privacy Rules also emphasise accountability, making accountability the emerging theme for global privacy governance.

The United States and Europe share a common data protection heritage

Privacy protection in the United States has its earliest roots in the Fourth Amendment of the US constitution. Prior to US independence, British soldiers routinely burst into the homes of citizens, which prompted the drafters of the US constitution to include a fundamental right to protection of the security of each individual's home against government intrusion. The Fourth Amendment is focused on intrusions by the government, not by private

1. Transfers are prohibited unless one of the exceptions applies: safe harbor, standard contractual clauses, binding corporate rules, etc.

actors. Although originally focused on the individual's home, the Fourth Amendment has been extended to other contexts where individuals have a reasonable expectation of privacy similar to what they would enjoy in their own home. For example, the Supreme Court recently held that the placing of a GPS tracking device on the outside of a car was the equivalent to a search of an individual's home which should have a search warrant. Another decision held that the use of police dogs to sniff around the outside of a home constituted a virtual search of the home, again requiring a search warrant. Wiretaps and certain other forms of electronic surveillance are also covered by the Fourth Amendment.

Because of sensitivity in the United States against privacy intrusions by the government, the United States enacted in 1974 a general law protecting individuals' personal data in the hands of the government. The Privacy Act of 1974 embodied the concept of FIPPs (Fair Information Privacy Practices) that originally were introduced in a report by the US Department of Health Education and Welfare. FIPPs later became the basis for the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which themselves formed the basis for the 1995 European Data Protection Directive.

In the late 19th century, US legal scholars began to recognise the need for privacy protection not only against the government, but against private parties who unreasonably invaded another person's private space. The much-cited Warren and Brandeis article, "The Right to Privacy,"[2] was prompted by the publication of photos in newspapers showing people in unflattering situations. The Warren and Brandeis article led to development of common law torts of privacy that protect various aspects of an individual's personal life and image. At about the same time as the Warren and Brandeis article, there were lawsuits in France dealing with the publication of unflattering photos in newspapers, which led to the enactment of a law in France, limiting publication of photos without an individual's consent.[3] Today, Article 9 of the French Civil Code recognises each person's right to his or her private life and image. This is similar to the four "privacy torts" defined by William Prosser in the US: (1) intrusion upon seclusion; (2) public disclosure of embarrassing private facts; (3) false light publicity; and (4) appropriation of name or likeness.[4]

In addition to the privacy torts, which are matters of state law, the United States has developed a series of statute-based laws dealing with personal

2. Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev., 1890. 193.
3. French press law of June 4, 1868.
4. William L. Prosser, *Privacy*, 48 Calif. L. Rev., 1960. 383, 383.

data in certain sectors. At the federal level, eight different privacy laws exist, each with a different acronym and scope of application:

– HIPAA (Health Insurance Portability and Accountability Act) – health data,
– GLBA (Gramm-Leach-Bliley Act) – financial data,
– COPPA (Children's Online Privacy Protection Act),
– FCRA (Fair Credit Reporting Act),[5]
– ECPA (Electronic Communications Privacy Act),
– VPPA (Video privacy protection act),
– Cable TV Privacy Act,
– "Can-SPAM" Act.

Some of these laws are at least as restrictive as European data protection laws, although their scope is more limited. In addition to these focused federal laws, there exists a myriad of state laws dealing with targeted privacy issues. The State of California is particularly active, having enacted laws targeting the collection of data via the Internet as well as the so-called "eraser" law, which permits minors to delete their personal data on Internet platforms.[6] California also has a general right of privacy included in the state's constitution. Almost all states in the United States have laws regulating how data breaches should be notified.

In addition to these focused statutes, the United States has a general statute on consumer protection that has been used extensively as a means to protect personal data. Section 5 of the Federal Trade Commission Act prohibits any unfair or deceptive practice and empowers the Federal Trade Commission (FTC) to enforce the provision against companies. Over recent years, the Federal Trade Commission has proactively expanded the concept of unfair and deceptive practice to include processing of personal data by companies in ways that do not match the reasonable expectations of consumers. The FTC's first point of focus is on the privacy policies that companies themselves publish. If any of the statements in the privacy policy are not respected by the company, either in spirit or in letter, the FTC will accuse the company of an unfair and deceptive practice. The FTC has expanded the concept of unfair and deceptive practice to cover information security, thereby putting a relatively high burden on companies to take measures to protect personal data against unauthorised disclosure. The FTC has a wide range of tools at its disposal, going from soft measures such as workshops and guidelines to more draconian measures such as sanctions and, importantly, settlement agreements. (We will return to the subject of settlement agreements in the second part of this article.)

5. Incidentally the FCRA includes a form of "right to be forgotten."
6. For a description of California's privacy laws, see, http://oag.ca.gov/privacy/privacy-laws.

The FTC uses these tools to send signals to the market regarding the FTC's interpretation of the vague "unfair and deceptive" standard. Professor Solove refers to the FTC's "new common law of privacy."[7] Many states have their own authorities (generally the attorney general), which enforce state privacy rules. Those state authorities can issue guidelines in addition to those of the FTC. The recent guidelines issued by the California Attorney General on mobile applications[8] contain recommendations that resemble in many respects the position of Europe's Article 29 Working Party.[9]

Even in matters involving government surveillance, US and European laws are not as far apart as they might seem. Like most European countries, the United States has a separate set of rules for normal police investigations and for national security operations.[10] Police investigations are governed by the "Crimes and Criminal Procedure"[11] section of the US Code, whereas national security investigations are governed by the "Foreign Intelligence Surveillance" and "War and National Defense"[12] sections of the Code. This is similar to the legal structure in France: the *Code de procédure pénale* governs surveillance in the context of criminal investigations, and the Code de la sécurité intérieure governs surveillance in the context of national security. As can be expected, the rules surrounding national security provide fewer safeguards and less transparency than the rules applicable to criminal investigations. In criminal investigations, police must obtain a court order before conducting intrusive surveillance. In national security matters, authorisations may be given by a separate national security court (in the US) or by a specially named person in the Prime Minister's office (in France).

The Snowden affair has raised serious questions about the adequacy of the US framework for national security surveillance. A recent report commissioned by President Obama shows that the US regime for collection of data in national security cases requires improvement, in particular to better protect privacy of both US and non-US citizens.[13] The European Commission also listed areas where the US could help restore trust in cross-border data flows, including the

7. Daniel Solove and Woodrow Hartzog, "The FTC's New Common Law of Privacy", August, 2013, www.ssrn.com.
8. California Attorney General, "Privacy on the Go, Recommendations for the Mobile Ecosystem", January 2013 http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.
9. Article 29 Working Party, Opinion n° 02/2013 on apps on smart devices, WP 202, February 27, 2013.
10. Winston Maxwell and Christopher Wolf, "A Global Reality: Governmental Access to Data in the Cloud", Hogan Lovells White Paper, May 2012.
11. Title 18, US Code, "Crime and Criminal Procedure."
12. Title 50, US Code, "War and National Defense."
13. "Liberty and Security in a Changing World", Report and Recommendations of the President's Review Group on Intelligence and Communications Technology, Dec. 12, 2013.

negotiation of an "umbrella agreement" with Europe regarding government surveillance.[14] The Snowden affair has also shown that the United States is not alone: intelligence agencies in major European countries conduct similar data collection practices with little or no court supervision.[15] The debate is therefore not "US versus Europe," but a more fundamental question of finding the appropriate balance between security and privacy in a data-centric age. Both security and privacy are fundamental rights. Without security, privacy cannot exist – security is an "enabler" of other fundamental rights.[16] By the same token, security cannot swallow privacy. Finding the right balance is not easy, and new data gathering techniques give these questions a new dimension and urgency. The Snowden affair has had the merit of bringing the issue to the forefront so that those debates can occur before national parliaments and courts.

We have seen a number of similarities between Europe and the United States, as well as common issues relating to government surveillance and fundamental rights. What are the main differences between the two frameworks? The differences have been examined in detail elsewhere.[17] Suffice it to say here that one of the key differences is philosophical: In the United States, certain areas of personal data are surrounded by strict safeguards (eg. HIPPA, GLBA). However, outside of those closely regulated areas, companies are free to exploit data as long as they do not commit an unfair consumer practice. In Europe, personal data is attached to a fundamental right. The starting point for analysis is that any exploitation of data potentially violates a fundamental right and must therefore have a compelling justification. Some data (eg. sensitive data) require a high level of justification, other data require less. But the starting point is that each individual has a personal right to control his or her personal data, and that processing by others is forbidden unless justified by a list of well-defined reasons. In practice, the US and European approaches often lead to the same practical result, but the reasoning begins from different points.

The US and Europe converge in co-regulation and accountability

Co-regulation is a system under which a state-sponsored institution, such as a government agency or independent regulatory authority, creates a frame-

14. European Commission Press Release: "European Commission calls on the US to restore trust in EU-US data flows", November 27, 2013, IP/13/1166.
15. See, e.g., Jacques Follorou and Franck Johannès, "*Révélations sur le Big Brother français*", *Le Monde*, July 5, 2013; Winston Maxwell, "Systematic government access to private-sector data in France", International Data Privacy Law 2014, Oxford, forthcoming.
16. In France, this principle was affirmed by the Constitutional Council in decision n° 94-352 DC of January 18, 1995 in connection with videosurveillance.
17. Christopher Wolf and Winston Maxwell, "So Close, Yet so far Apart: The EU and US Visions of a New Privacy Framework", *Antitrust*, Vol. 26, no 3, 2012.

work within which private actors discuss and if possible agree on regulatory measures. Co-regulation is like self-regulation, except that in co-regulation the government or regulatory authority has some influence over how the rules are developed, and/or how they are enforced. This is supposed to make the rulemaking process more legitimate and effective compared to purely self-regulatory solutions. It is more legitimate because the process is supervised by officials who are accountable to the democratically-elected legislature. It is more effective because the resources of the state can be used to enforce the rules.

Data protection authorities in Europe are distrustful of purely self-regulatory arrangements, and prefer co-regulatory solutions in which the data protection authority (DPA) is involved in both the formation of rules and their enforcement. DPAs in Europe emphasise binding corporate rules (BCRs), which evidences this co-regulatory preference.

Under the European data protection directive, companies are prohibited from sending personal data outside the EEA to countries that have not been recognised by the European Commission as providing an adequate level of data protection. The United States currently is not viewed as providing an adequate level of protection of personal data. One of the ways companies can overcome the prohibition is by adopting BCRs. BCRs are a set of internal procedures that guarantee a high level of protection of personal data throughout the organisation, including in parts of the organisation located in countries without "adequate" protection. BCRs must be developed in close cooperation with DPAs in Europe. A multinational group can propose BCRs following a template adopted by the Article 29 Working Party, but ultimately the content of the BCRs must be negotiated point by point with one of Europe's DPAs. Once the lead authority is satisfied with the content of the BCRs, the file is then sent to two other co-lead DPAs who in turn scrutinise the content of the file to ensure that the BCRs meet European standards. Once the BCRs have been approved, they confer rights on third parties who can sue the company for any violation of the BCRs. Likewise, any breach of the BCRs can give rise to sanctions by DPAs.

BCRs constitute co-regulations because they are developed by private stakeholders within a framework established by regulatory authorities, and once they have been adopted, the BCRs can be enforced by regulatory authorities in the same way as classic regulations.

The Federal Trade Commission's (FTC) extensive reliance on negotiated settlement agreements can also be seen as a form of co-regulation. The FTC conducts investigations and begins enforcement action against companies that have violated the "unfair and deceptive practices" rule, as well as

other privacy violations such as violation of the US-EU safe harbor framework. One of the procedural options that the FTC can propose is a settlement agreement with the company, which binds the company to put an end to the relevant practices as well as submit itself to on-going accountability obligations similar to those one sees in BCRs.

The individual settlement agreements provide for procedural and structural safeguards to help prevent violations of data privacy commitments.[18] Like European BCRs, the negotiated settlement agreements provide for both internal and external audit procedures, training programs and periodic reporting to the FTC. The settlement agreements last for 20 years, giving the FTC the ability to co-regulate major Internet companies over a long period of time. The FTC settlement agreements are public, thereby permitting the FTC to use the settlement agreements as a means of sending signals to all companies in the relevant sector. Although the settlement agreements are not binding on companies that are not signatories, the settlement agreements provide to third parties guidance on what the FTC considers to be the state of the art in terms of privacy compliance. The settlement agreements inform third parties on practices that the FTC is likely to view as unacceptable, as well as compliance measures that the FTC is likely to consider as optimal.

The FTC settlement agreements can have wide ranging effects. First, if the settlement agreement binds a major Internet platform such as Facebook, the settlement agreement will have an impact on a large portion of the Internet industry simply because the platform represents a large part of Internet users. Second, the settlement agreement will have indirect effects on all other players in the Internet industry, by showing best practices and FTC expectations. The FTC's settlement agreements serve a pedagogical function, thereby contributing to overall compliance with regulatory best practices in the industry.

The United States government is trying to encourage other co-regulatory solutions for data privacy. The US administration refers to this as the "multi-stakeholder process." Under the multi-stakeholder process, the National Telecommunications and Information Agency, the NTIA, convenes stakeholders in an effort to develop codes of conduct. The role of the NTIA is to organise multi-stakeholder meetings, facilitate the exchange of information, and apply the threat of mandatory regulatory measures should the stakeholders fail to agree on consensual measures. The NTIA acts as a maieutic regulator,[19] helping to nudge stakeholders toward a consensus. The presence

18. For an example, see the Facebook settlement agreement here: http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.
19. Nicolas Curien, "Innovation and Regulation serving the digital Revolution", *The Journal of Regulation*, 2011, I-1.32, p. 572-578.

of the government in the discussion also ensures that the self-regulatory measures that emerge from the discussions satisfy public interest objectives, and in particular, the protection of privacy rights. The multi-stakeholder process recently yielded draft recommendations on transparency in mobile applications.[20]

The emphasis on co-regulation is not surprising given the emphasis on accountability in the 2013 OECD Guidelines, the proposed European Data Protection Regulation, the APEC Privacy Framework and in the White House's Consumer Privacy Bill of Rights.[21] Accountability amounts to internal privacy compliance programs implemented by companies that then create legally binding rights and obligations – a form of co-regulation.

The convergence of US and EU co-regulatory philosophies will be tested in connection with efforts to create a compatibility system between European BCRs and Cross Border Privacy Rules (CBPR) developed under the APEC framework.[22] Like BCRs, CBPRs represent a set of data protection obligations that companies can subscribe to, and that will be enforced by data protection authorities in participating APEC countries. Application of the rules is verified by an "accountability agent."[23] The purpose of subscribing to the CBPRs is to demonstrate compliance with the APEC Privacy Framework principles,[24] and thereby facilitate data flows among APEC economies. An international group that successfully implements both BCRs and CBPRs would meet accountability obligations under both EU and APEC frameworks. Accountability is therefore becoming the pillar of an emerging global privacy governance model.

Winston Maxwell *is a partner with the international law firm Hogan Lovells, and is recognised as one of the leading media, communications and data protection lawyers in France. Winston Maxwell is a co-author of* La Neutralité d'Internet *(La Découverte, 2011) as well as numerous articles on Net neutrality, data protection law, and telecommunications regulatory issues. Winston Maxwell teaches courses on data protection and regulation of the digital economy at Télécom Paristech and HEC in France, and advises both regulators and corporate clients on Internet, data protection, media and telecom regulatory matters. He received his law degree in 1985 from Cornell Law School and is admitted to practice law before both the Paris and New York bars.*

20.http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.
21. United States White House, "Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy", February 2012.
22. http://www.apec.org/Press/News-Releases/2013/0306_data.aspx.
23. For a full description of CBPRs, see http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.
24. http://publications.apec.org/publication-detail.php?pub_id=390.