Published in TELOS, Revista de Pensamiento sobre Comunicación, Tecnologia y Sociedad
February-May 2014

Restoring Trust across the Atlantic[*]

Peter Hustinx[**]
European Data Protection Supervisor

The recent stream of revelations about mass surveillance on the Internet by US and other security services has created shock waves around the world, but also exposed a serious multi-layered problem between the EU and the US. Not only have we now learned about excessive, wide spread and structural surveillance of all citizens going about their daily business, but this mass surveillance is tapping into an infrastructure of free services, often dominated by US companies, where citizens' personal data are continuously monitored and turned into huge profits in advertising across the Internet. This infrastructure has developed gradually over a decade, with some obvious popular support, but with very little public awareness of consequences that have now become visible. Moreover and importantly, there is also a worrying lack of balance between the applicable legal frameworks at both sides of the Atlantic.

The European Commission has recently presented an action plan for rebuilding trust in EU-US data flows[1]. This action plan also calls on the US government to contribute its share in restoring trust and bridging the current divide. However, it is important to realise that the problems which have emerged, have deep roots in history and legal culture, and that addressing them will be a long term process. In any case, it is best to

---

[*] Published in TELOS, Revista de Pensamiento sobre Comunicación, Tecnologia y Sociedad, nr. 97, February-May 2014, p. 80-82.
[**] Mr Hustinx is European Data Protection Supervisor (EDPS). Email contact: edps@edps.europa.eu; Website: www.edps.europa.eu
[1] Communication from the Commission to the European Parliament and the Council, *Rebuilding Trust in EU-US Data Flows*, 27 November 2013, COM(2013) 846 final

treat the issue of 'excessive spying' separately from the other, more structural issues, although we should be aware of the connections.

There is also some common ground between the EU and the US. The first ideas on the protection of personal data emerged, both in the EU and the US, at the same time, in the early 1970s. The principles set out in the Council of Europe Convention on Data Protection (1981) were in fact based on the US Fair Information Principles[2] that also inspired the OECD Privacy Guidelines (1980). However, subsequent developments took a different course: while the US, apart from some specific laws, mostly relied on self-regulation, the EU continued to invest in a framework of national laws, within the scope of Directive 95/46/EC. This eventually led to the recognition of the right to the protection of personal data as a separate fundamental right in Article 8 of the Charter of Fundamental Rights, made binding in the Lisbon Treaty at the end of 2009.

However, behind this difference in legal infra-structure is an important constitutional difference. The 4th Amendment to the US Constitution - prohibiting unreasonable searches and seizures[3] - has a much narrower scope than the right to the respect for private life, as set out in Article 7 of the EU Charter[4]. As a result, the 4th Amendment only applies to *content* and not to other communication data - such as caller, time and location - and in principle only protects US citizens. Moreover, information entrusted to a service provider, no longer benefits from its protection, while the starting point in EU law still lies in the confidentiality of communications.

Over the years, creative solutions have been found to bridge the gap between EU law and US self-regulation. A good example is the Safe Harbour decision[5], allowing data transfer from the EU to US companies which have undertaken to comply with Safe Harbour principles, subject to jurisdiction by the US Federal Trade Commission under the US Fair Trade Act. Although by now more than 3000 companies have joined the arrangement, some key problems continue to exist and the Commission[6] has identified 13 points for improvement and announced a thorough review by the summer of 2014.

---

[2] US Department of Health, Education and Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens* (Washington DC 1973)

[3] Amendment IV to the US Constitution: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"

[4] Article 7 of the Charter: "*Everyone has the right to respect for his or her private and family life, home and communications*".

[5] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p.7.

[6] See Communication mentioned in footnote 1.

Meanwhile, the EU has invested much energy in a thorough review of its existing legal framework for data protection in order to make it stronger and more effective in view of the challenges of new technologies and globalisation.[7] This will provide stronger rights for data subjects, stronger responsibilities for data controllers, and stronger supervision and enforcement by independent authorities. The proposal for a General Data Protection Regulation[8] - directly binding in all Member States - will ensure greater consistency of legal rules and practices across the European Union. A strong framework with clear rules that are enforceable also in situations where data are transferred abroad is now - more than ever - a necessity.

An important aspect of this proposal is that it will apply to all companies active on the European market, regardless from where they are operating. The new framework will thus also apply to companies established in the US or other third countries, which are not subject to similar rules in their own country. This will probably also include well known operators on the Internet that may have been subject to mass surveillance, while serving EU consumers. The new rules will provide an instrument against undue practices of companies, now engaged in systematic monitoring and exploitation of consumer behaviour. The sheer size of the European market will help to make this a realistic option.

The new rules might also provide for a mechanism[9], so as to address the possibility of a conflict of (inter)national law, where jurisdictions have conflicting views of their public interests. The basic principle should be that all data flows must be in line with EU law, unless a binding international agreement has provided otherwise, or a judicial or supervisory authority has granted an exemption. Such a mechanism might be useful in different situations, including those now possibly affected by mass surveillance.

In this context, it is relevant that the action plan recently presented by the European Commission also provides for steps in the context of international agreements with the US.[10] Apart from the Safe Harbour arrangement, already briefly touched upon, the Commission aims at strengthening data protection safeguards in the law enforcement area. This involves the conclusion of an agreement for transfers of data in the context of police and judicial cooperation, with a high level of protection for citizens at both sides of the Atlantic. This also means that EU citizens, not resident in the US, should

[7] See the Reform Package presented by the European Commission in January 2012.

[8] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final

[9] See amendments adopted by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) on 21 October 2013.

[10] See Communication mentioned in footnote 1.

benefit from judicial redress mechanisms. Data transfer for law enforcement purposes should use official channels. Asking data from EU companies directly should only be possible in clearly defined, exceptional and judicially reviewable situations.

The European Commission also insisted that European concerns should be addressed in the ongoing US reform process. This refers to the review of US national security authorities' activities, including of the applicable legal framework, announced by President Obama. The most important changes, envisaged by the Commission, would be extending the safeguards available to US citizens and residents, to EU citizens not resident in the US, increased transparency of intelligence activities, and strengthening oversight of these activities. The necessity and proportionality of current surveillance programmes should also be carefully considered.

The European Commission also mentioned the increasing need for international privacy standards, particularly on the Internet. In this context, it referred to several recent initiatives, such as the draft resolution for the UN General Assembly proposed by Germany and Brazil, building on Article 17 of the International Covenant on Civil and Political Rights (1966) and calling for the protection of privacy online and offline.

Data exchanges across the Atlantic and beyond would also greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections.[11] The existence of strong and enforceable data protection rules enshrined in the EU and the US would indeed provide a more solid basis for cross-border data flows.

Finally, it should not be ignored that EU Member States may have played or may still be playing an important role in the issue of mass surveillance. The fact that national security is the sole responsibility[12] of each Member State is in any case not a good reason to avoid raising the right questions and taking the right measures, at the earliest moment and at the appropriate levels.

[11] See: *"Consumer Data Privacy in a Networked World: a framework for protecting privacy and promoting innovation in the global digital economy"*, February 2012, Washington DC.
[12] See Article 4(2) of the Treaty on European Union (TEU)