With its Systemic Remedies, "the US Now Serves as a Baseline for Foreign Intelligence Standards"

Conclusion of team led by Oxford Professor Ian Brown after comparing US safeguards to other countries

By Peter Swire

This essay is part of a five-part series that highlights critical issues in my 300-page testimony that explains U.S. surveillance law and related issues in the Standard Contracts Clause case before the Irish High Court concerning data flows between the US and the EU. An overview of the testimony can be found at **www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony**.[1]

The Irish High Court is currently considering whether Standard Contract Clauses (SCCs) will continue to be considered a valid basis for transfer of personal data between the EU and the US. The court has shown a particular interest in the surveillance practices of the US government.

As described in detail in my testimony, the US has developed multiple ways to ensure oversight by persons with access to classified information for the necessarily secret activities, and to create transparency in ways that do not compromise national security. In my view, the US system provides effective checks against abuse of secret surveillance powers – which is superior to any that I am aware of in the world.

I agree with the team led by Oxford Professor Ian Brown, who after comparing US safeguards to other countries, concluded that "the US now serves as a baseline for foreign intelligence standards," and that the legal framework for foreign intelligence collection in the US "contains much clearer rules on the authorisation and limits on the collection, use, sharing and oversight of data relating to foreign nationals than the laws of almost all EU Member States."[2]

Systemic Safeguards for Foreign Intelligence

[1] Swire is the Elizabeth and Thomas Holder Chair and Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business, and Senior Counsel at Alston & Bird. Swire's expert report was submitted to the Irish High Court in the current litigation where Max Schrems is challenging whether transfers of personal data under Standard Contract Clauses are adequately protected under European Union privacy law. Under Irish rules, Swire was an expert selected by Facebook, but required to give his independent opinion about U.S. law, and Swire retained complete editorial control over the content of the testimony. The decision to make the report public was made by Swire, and was not the decision of Facebook. The full report is available **here**, with other explanatory material **here**.

[2] Ian Brown et al., *Towards Multilateral Standards for Surveillance Reform* (2015), https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf. Chapter 6 of the testimony examines the Brown study in detail, comparing the safeguards in the US and other countries.

Many of the most effective protections for privacy, in my experience, exist at the *systemic* level, rather than occurring primarily on a retroactive basis through an individual remedy.[3] An analogy I discussed at trial helps illustrate the relative importance of systemic safeguards compared with after-the-fact individual remedies. In the area of automobile safety, it is of course important to have individual tort remedies to provide redress after the fact in the case of an accident. Focusing only on these after-the-fact individual remedies, however, misses the much larger goal – providing safe cars and preventing the accidents from occurring. The argument is that protection comes in large measure by building safe cars (systemic remedies), rather than focusing exclusively on legal action after an accident (individual right to redress). The Irish Data Protection Commissioner, in the pending case, relied solely on concerns about the lack of after-the-fact individual remedies. She cited only the remedies provisions of Article 47 as the basis for finding a lack of adequacy. By contrast, the car analogy reminds us that the goal is overall protection of individual rights, and not simply the ability to have an individual cause of action after violations have occurred.

Chapter 3 of my testimony provides a detailed explanation (49 pages) documenting systemic protections under U.S. law for foreign intelligence surveillance. Under U.S. law, the most fundamental systemic remedies arise from the US Constitution, which created a time-tested system of checks and balances among the three branches of government and has been in continuous operation since 1790. For government access to personal data, the Fourth Amendment to the US Constitution plays a particularly important role. The jurisprudence concerning the Fourth Amendment has responded to changing technology.[4] Other constitutional protections for information about a person's information include: the First Amendment,[5] the Third Amendment,[6] and the Fifth Amendment.[7] These constitutional rights, enforced by independent judges, provide systemic protections against over-reach by the other branches of government.

---

[3] *See* Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306 (2004). Chapter 2 of the testimony documents ten reform proposals from that article that have since been implemented.

[4] Federal courts in recent years have issued a string of Fourth Amendment rulings to protect privacy, such as *Riley v. California* (warrant needed to search cell phones), *United States v. Jones* (warrant needed when attaching a GPS device to a car), *Kyllo v. United States* (warrant needed for high-technology search of home conducted from the street), and *United States v. Warshak* (warrant needed to access email).

[5] This amendment protects free speech, assembly, and association, providing a wide range of protections against government interference with freedom of thought and expression. With regards to privacy, the First Amendment protects a range of anonymous speech. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995). It also protects the right of individuals to gather or communicate privately. LEGAL INFORMATION INSTITUTE, *First Amendment: An Overview*, https://www.law.cornell.edu/wex/first_amendment.

[6] Because soldiers had been quartered in homes during colonial times, the Founders specifically outlawed this practice under the Constitution. This protection supports the privacy of one's home. William Sutton Fields, *The Third Amendment: Constitutional Protection From the Involuntary Quartering of Soldiers*, 124 MIL. L. REV. 195 (Spring 1989).

[7] The prohibition on compelled self-incrimination protects the privacy of an individual's thoughts. In the context of electronic evidence, this provision of the US Constitution has been used to restrain the government from requiring an accused person from providing passwords and encryption keys. *See, e.g.*, *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, U.S. v. John Doe*, 670 F.3d 1335, 1352 (11th Cir. 2012), http://stanford.edu/~jmayer/law696/week8/Compelled%20Password%20Disclosure%20(Eleventh%20Circuit).pdf.

In addition to constitutional checks, major safeguards in the US system of foreign intelligence law are codified in statute. Most notably, in 1978, the US Congress passed the Foreign Intelligence Surveillance Act (FISA).[8] Following the Snowden disclosures, Congress in the USA FREEDOM Act of 2015 strengthened important aspects of FISA, and ended bulk collection under Section 215 of the PATRIOT Act.[9]

My testimony in December 2015 to the Belgium Privacy Agency discussed 24 distinct surveillance reforms that the United States undertook from the time of the Edward Snowden disclosures in 2013 through the time of the testimony.[10] Between 2013 and the filing of my testimony in Ireland in November 2016, there were important additional reforms, notably the Privacy Shield, the Judicial Redress Act, and the Umbrella Agreement on law enforcement sharing. The 2015 testimony discussed these reforms:

-*Independent reviews of surveillance activities*

1. Review Group on Intelligence and Communications Technology;
2. Privacy and Civil Liberties Oversight Board (PCLOB);

-*Legislative actions*

3. Increased funding for the PCLOB;
4. Greater judicial role in Section 215 orders;
5. Prohibition on bulk collection under Section 215 and other laws;
6. Declassification of FISC decisions, orders, and opinions;
7. Appointment of experts to brief the FISC on privacy and civil liberties;
8. Transparency reports by companies subject to court orders;
9. Transparency reports by the US government;
10. The Judicial Redress Act;

-*Executive branch actions*

11. New surveillance principle to protect privacy rights outside of the US;
12. Protection of civil liberties in addition to privacy;
13. Safeguards for the personal information of all individuals, regardless of nationality;
14. Retention and dissemination limits for non-US persons similar to US persons;
15. Limits on bulk collection of signals intelligence;
16. Limits on surveillance to gain trade secrets for commercial advantage;
17. White House oversight of sensitive intelligence collections, including of foreign leaders;
18. White House process to help fix software flaws rather than use them for surveillance;

[8] *See* 50 U.S.C. § 1801 *et seq.*

[9] *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23 (2015).

[10] Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, https://ssrn.com/abstract=2709619.

19. Greater transparency by the executive branch about surveillance activities;
20. Creation of the first NSA Civil Liberties and Privacy Office;
21. Multiple changes under Section 215;
22. Stricter documentation of the foreign intelligence basis for targeting under Section 702 of FISA;
23. Other changes under Section 702; and
24. Reduced secrecy about National Security Letters.

This year, the NSA announced another reform – the agency ended a portion of its Upstream program known as "about" collection.[11]

Systemic Safeguards in Law Enforcement Investigations

In addition to foreign intelligence, the US has a system of safeguards protecting individuals in the context of criminal investigations. Chapter 4 of the testimony describes multiple areas where US criminal procedure safeguards are stricter (more substantial) than other countries, including: strict judicial oversight;[12] stricter oversight for interceptions;[13] penalties for illegal searches;[14] orders permitting legal challenges;[15] no mandatory data retention;[16] and strong encryption.[17] An expanded version of that analysis recently appeared in an Emory Law Journal article.[18]

---

[11] "About" collection can best be thought of in contrast to the collection of email that is sent "to" and "from" the email address of a foreign intelligence target. An email communication would be retained as part of "about" collection if the body of the email contained the targeted email address, even though the persons that the email is send "to" and received "from" are not targeted themselves.

[12] Independent judicial officers oversee applications for warrants to conduct searches and collect evidence. "Probable cause," the requirement for granting a warrant to search, is a relatively strict requirement for digital searches. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), https://scholar.google.com/scholar_case?case=11707608375476732 55&hl=en&as_sdt=6&as_vis=1&oi=scholarr.

[13] Telephone wiretaps and other real-time interception have even stricter requirements, such as successive rounds of agency review, minimization safeguards for non-targets, and requirements to exhaust other sources of information. *See* 18 U.S.C. § 2518.

[14] The so-called "exclusionary rule" bars evidence obtained through an illegal search from being used at criminal trials, while the "fruit of the poisonous tree" doctrine further bars additional evidence derived from the illegal search. Officers who conduct illegal searches are subject to civil damages lawsuits. *See Mapp v. Ohio*, 367 U.S. 643 (1961); *Wong Sun v. U.S.*, 371 U.S. 471 (1963); *Bivens v. Six Unknown Agents*, 403 U.S. 388 (1971); 42 U.S.C. §1983.

[15] US law requires court orders to clearly indicate the legal basis for a warrant or information request, permitting the recipient to determine whether there is a basis to challenge the order. *See* 18 U.S.C. § 2703(b).

[16] US law does not require data retention for Internet communications, such as email. For telephone communications, US law requires limited retention of records needed to resolve billing disputes. *See* 47 C.F.R. § 42.6.

[17] The US permits the use of strong encryption, a privacy-preserving technology, which has been widely adopted by US-based technology companies. *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416 (2012).

[18] Peter Swire & DeBrae Kennedy-Mayo, "How Both the EU and U.S. are 'Stricter' Than Each Other for the Privacy of Government Requests for Information, 66 Emory L.J. (2016).

In conclusion, I agree with the Oxford team's determination that the EU Member States' legal frameworks for foreign intelligence "generally compare unfavorably with the situation in the US" after the adoption of Presidential Privacy Directive 28. The Oxford team pointed out that European governments that want to further limit the NSA's activities concerning EU citizens first "need to get their own houses in order by developing, publicizing, and adopting publicly available standards that govern foreign intelligence collection."[19]

[19] Ian Brown et al., *Towards Multilateral Standards for Surveillance Reform*, 10-11 (2015), https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf.