The US Has an Extensive and Often Under-Appreciated Set of Remedies for Privacy Violations

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 will continue to be considered a valid basis for transfer of personal data between the EU and the US. When the Irish Data Protection Commissioner referred the case to the Court, the central question was whether the US system provides sufficient individual remedies for privacy violations.

Chapter 7 of my testimony documents how the US legal system provides numerous ways for an individual to remedy violations of privacy. The chapter draws on the textbook on US private-sector privacy law of approximately 200 pages that I have written for the International Association of Privacy Professionals, with a new and expanded edition scheduled to be released this year.[2]

This essay summarizes the multiple ways that remedies exist under the US legal system. US law provides important remedies for individuals where companies violate privacy laws. Individuals can seek the assistance of the Federal Trade Commission and other federal agencies where violations exist. State laws also protect privacy, and the US civil litigation system offers many advantages for plaintiffs compared with other legal systems, including widespread use of class actions for privacy violations.

Remedies Against Companies for Privacy Violations

Individuals have important remedies against companies, such as Facebook, if they improperly turn over communications to law enforcement or national security agencies. Under the Stored Communications Act, individual data subjects may bring a civil action in federal court for unlawful disclosure of personal data.[3] The plaintiff can obtain preliminary relief (e.g.,

---

[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**. Justin Hemmings was the principal attorney assisting me for these two chapters.

[2] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS (2012).

[3] 18 U.S.C. § 2707.

injunctions) where appropriate, actual damages in an amount of no less than $1,000 USD per person (with an option for punitive damages where the violation was "willful"). Claimants can also recover court costs and attorney's fees, where appropriate. Similar individual suits are permitted under the Wiretap Act. Both laws enable any aggrieved person, including an EU data subject, to exercise the right of action.[4] The statutory damages of $1000/person create a powerful incentive for service providers to comply with the law – an illegal surveillance program involving one million people exposes the company to suit for $1 billion damages.[5]

Along with these direct lawsuits by individuals, federal agencies such as the Federal Trade Commission, Federal Communications Commission, Consumer Financial Protection Bureau, Securities and Exchange Commission, and Department of Health and Human Services all serve as active privacy enforcers, with leading enforcement cases documented in the testimony. Individuals can and do complain to these agencies about privacy violations, similar to complaints made to EU Data Protection Authorities. The agencies can then bring actions, often with substantial penalties, against companies that fail to comply with applicable law or company privacy policies, such as when the companies improperly provide electronic communications to the government.

Part IV of Chapter 7 explains the role of state law, State Attorneys' General, and other private rights of action in providing privacy remedies. Award-winning research by Professor Danielle Citron has recently documented the leading role of State Attorneys' General in providing remedies for privacy violations.[6] State law often provides individual private remedies that go beyond federal statutes, and the testimony surveys, as an example, a wide range of laws in the state of California that provide such individual remedies.

The testimony also reviews five major reasons that US law is generally seen as more favorable to individual remedies than in other jurisdictions:

1. Attorney's fees. The US rule generally requires each party to pay its own costs, lowering the bar for individuals to sue large corporations.
2. Contingency fees. This practice enables US plaintiff law firms to take on clients who otherwise would lack the resources to sue for privacy or other violations.
3. Jury trial. Plaintiffs' lawyers often prefer a jury trial, composed of citizens, to decisions by a judge.
4. Broad discovery. Plaintiffs can often begin a case with a relatively small number of supporting facts, and develop the case in the course of discovery.
5. Class actions. US law has more favorable rules for class actions than other nations, so that a single data breach or privacy violation can lead to a lawsuit involving thousands or even millions of consumers.

---

[4] *Id.* § 2707(a); *Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf.

[5] Peter Swire, *Questions and Answers on Potential Telco Liability*, THINK PROGRESS (May 12, 2006), https://thinkprogress.org/questions-and-answers-on-potential-telco-liability-e5fa4bdd4c0d#.1qokc850w.

[6] Danielle Keats Citron, *Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

As empirical support for the claim that US courts have supported privacy remedies, the testimony documents class-action privacy settlements totaling over $425 million to plaintiffs and government agencies in the past ten years.

Conclusion

Chapter 7 of the testimony thus summarizes numerous and significant ways that remedies are available in the US legal system for privacy violations. Along with the individual, agency, and class-action remedies summarized here, US law provides a range of criminal and civil laws that the US Department of Justice can invoke for privacy violations, including for disclosure of service provider records. In response to concerns raised by the EU, the Judicial Redress Act, Privacy Shield, and Umbrella Agreement with the EU have provided supplemental privacy remedies. There is also a range of press, civil society, oversight agency, and other mechanisms for uncovering privacy violations and remedying them. The overall high level of compliance has been documented by scholars -- Professors Kenneth A. Bamberger and Deirdre K. Mulligan's book *Privacy on the Ground* studied corporate behavior in five countries, and found that US companies often have stronger privacy management practices than in EU countries.[7]

In the current litigation in Ireland, an important issue has been whether the US does (or should, under EU law) have sufficient remedies for any violations of foreign intelligence surveillance rules. Chapters 3 and 4 of the testimony explain that the most effective protection against privacy violations often comes from implementing "systemic safeguards" – established practices that prevent violations from occurring rather than focusing only on after-the-fact lawsuits. Chapter 8 of the testimony addresses a related issue, whether it is required under EU law for individuals to have access to records about them held by the foreign intelligence services of other nations. The discussion there explains the serious national security risks that would arise from such an approach, because of the exposure of the intelligence agencies sources and methods.

Taken together, the testimony supports the view that the US has extensive and effective remedies for privacy violations, as well as a world-class set of systemic safeguards, and a necessary and proportionate exception with respect to individual access to national security information. .

[7] *See generally* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).