

# The U.S. System of Safeguards for Foreign Intelligence Investigations is Effective

*A finding of inadequacy could have sweeping ramifications for EU/US trade and more broadly*

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. Materials for my testimony can be found at [www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony](http://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony).<sup>1</sup>*

In the current case, the Irish High Court is considering whether Standard Contract Clauses will continue to be a lawful basis for transfer of personal data from the EU to the US. Max Schrems, in his complaint to the Irish Data Protection Commissioner and on appeal, questioned whether there are adequate safeguards against surveillance by the US government for data transferred to the US. The Irish Data Protection Commissioner referred the case to the High Court, finding Mr. Schrem's allegation to be "well founded."

In 2015, in the first *Schrems* case, the European Court of Justice struck down the EU/US Safe Harbor Agreement as a legal basis for transferring data between the EU and the US, in significant part based on concerns about US surveillance practices. Later that year, I testified at the invitation of the Belgian Privacy Authority about the multiple and significant reforms of US surveillance law that occurred after the Snowden revelations, which began in 2013.<sup>2</sup> When the SCC case later came before the Irish High Court, I was asked by Facebook to serve as an expert witness on US surveillance law. Under Irish rules, I was selected by a party to the case (Facebook), and Facebook wrote me a letter setting forth the scope of requested testimony. I was required to be an independent expert, however, and I retained complete editorial control over the content of my testimony.

---

<sup>1</sup> 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](#). Attorneys at Alston & Bird supported my work on the testimony, led by James Harvey with lead assistance from Dan Felz, Justin Hemmings, DeBrae Kennedy-Mayo, and Suzanne Vergnolle.

<sup>2</sup> Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013," available at <https://ssrn.com/abstract=2709619>.

The result was my testimony of over 300 pages, essentially explaining US surveillance law to a non-US audience. The testimony drew on my longstanding work on US surveillance law, including as one of five members of President Obama’s Review Group on Intelligence and Communications Technology. It also drew on many years of work on EU data protection law, including a 1998 book on the topic and participation in negotiation of the 2000 Safe Harbor agreement.<sup>3</sup>

This essay provides an overall summary of my testimony. I am also posting four additional essays on specific aspects of the testimony:

1. **US systemic remedies.** As found by a team of Oxford experts, “the US now serves as a baseline for foreign intelligence standards.” Chapter 3 of the testimony provides a detailed explanation documenting systemic protections under US law for foreign intelligence surveillance. Chapter 4 documents strong safeguards for law enforcement surveillance. Based on the Oxford study, Chapter 6 shows how well the US safeguards compare with EU safeguards.
2. **US individual remedies.** Chapter 7 documents how the US legal system provides numerous ways for an individual to remedy violations of privacy, including individual suits against service providers, Federal Trade Commission and other agency enforcement, state law protections, and class action litigation. Chapter 8 explains reasons for a national security exception to individual access to surveillance records, where such access would threaten national security by revealing sources and methods.
3. **Foreign Intelligence Surveillance Court oversight.** Chapter 5 presents original research – research of all of the FISC opinions and related materials that were declassified between 2013 and the filing of my testimony in November 2016. The overall conclusion is that the FISC provides far stronger oversight than many critics have alleged – my opinion to the Irish court is that the FISC provides independent and effective oversight over US government surveillance.
4. **Broader implications of the SCC case.** Standard contract clauses are used pervasively for transfers of personal data out of the European Union. An inadequacy finding in the current case would have a great impact even if the finding applies only to a single country (transfers to the US) under a single basis for cross-border data flows (SCCs). Chapter 1 of the testimony, however, explains why an inadequacy finding in this case likely would have far greater implications. The implications appear greater geographically, as shown by analysis of surveillance rules in the BRIC countries – Brazil, Russia, India, and China. For those and other countries whose safeguards are less than in the US, it would appear that a finding of inadequate protections in the US would logically mean that transfers from the EU to these countries would similarly be prohibited. The testimony also explains why an inadequacy finding for SCCs may also apply to other legal bases for transfer of personal data, including Privacy Shield and Binding Corporate Rules. Taken together, a finding of inadequacy in the current case in Ireland could have far more sweeping ramifications than many observers have contemplated.

---

<sup>3</sup> Chapter 2 of the testimony sets forth my relevant background, including with a list of surveillance safeguards proposed in my earlier writings and now implemented by the US.

In conclusion, the EU Commission has emphasized the economic importance of transborder data flows between the EU and US by stating the economic relationship – the world’s largest – accounts for “nearly one trillion dollars in goods and services trade, . . . supporting millions of jobs on both sides of the Atlantic.”<sup>4</sup> The Commission has also stated that data flows “are an important and necessary element” of the strategic alliance between the EU and the US as “a crucial component of EU-US co-operation in the law enforcement field” and “in the field of national security.”<sup>5</sup>

The testimony provides an independent, detailed, and comprehensively footnoted record for consideration by the Irish High Court. The testimony can inform broader policy debates about the nature of US surveillance and European data protection law. It can also be of service in other pending litigation, such as current challenges to the Privacy Shield. Many surveillance reforms have been implemented since 2013, including the new protections in the USA-FREEDOM Act passed by Congress in 2015. I hope this testimony can inform the public debate on these vital issues.

---

<sup>4</sup> EU-U.S. PRIVACY SHIELD, Annex I.1., at 1, [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL).

<sup>5</sup> European Commission, *Communication from the Commission to the European Parliament and the Council*, COM (2013) 846, at 2 (Nov. 27, 2013), [http://ec.europa.eu/justice/data-protection/files/com\\_2013\\_846\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf).