Materials Prepared for "Data Protection: Global Convergence or Roads Diverged?"

ABA Section of Antitrust Law
Spring Meeting, March 2017

Peter Swire

Senior Counsel, Alston & Bird LLP

Huang Professor of Law and Ethics
Georgia Tech Scheller College of Business

These materials highlight challenges in how to reconcile different legal regimes for data protection, notably between the European Union and the United States. The EU in many respects has stricter protections for personal privacy than the US, especially concerning private-sector processing of personal data. (The comparison for protections against government access to data is more complex, with the US often having stricter protections.) These materials briefly explain three ways that EU and US legal regimes can interact, by: harmonization; inter-operability; or lack of express legal agreement.

(A) Background. I have worked on these EU-US privacy issues since the 1990's, when I was lead author of a book from Brookings called "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive." When serving as Chief Counselor for Privacy in the Office of Management of Budget, under President Clinton, I helped negotiate the EU-US Safe Harbor, which until it was struck down by the European Court of Justice in 2015 was a principal mechanism for transferring personal data from the EU to the US.

More recently, while continuing to work on these issues for private-sector data flows, in my role as Senior Counsel at Alston & Bird, much of my writing has focused on whether the US has "adequate" privacy protections under EU law in connection with surveillance by the National Security Agency. In 2013, I served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Based in part on that report's recommendations, President Obama in 2014 issued Presidential Policy Directive 28, which established privacy and civil liberties protections in U.S. signals intelligence for the citizens of EU and other nations. In February, 2017 I testified as an independent expert for the Irish High Court in the challenge by Max Schrems to the standard contract clauses used by many companies to transfer personal data from the EU to the US and other countries.[1] My conclusion was that

[1] I was selected to act as an expert by Facebook; under Irish rules, my responsibility was to testify as an independent expert for the court, and not on behalf of any party.

the US has protections for personal data with respect to intelligence agencies that are equivalent to, and often stronger than, protections in the EU.

(B) Harmonization, Inter-operability, and Potential Conflict Between Regimes. In thinking about how to reconcile the EU and US privacy regimes, in my experience it is useful to think of three categories for how the regimes can relate: harmonization, inter-operability, and lack of express legal agreement.

(1) Harmonization. One possibility is to formally harmonize the legal rules in the two regimes. Some writers have suggested a treaty approach, where the US and EU would agree on a set of rules that would apply on both sides of the Atlantic. A variation would be for the US to adopt comprehensive privacy legislation, tracking the numerous requirements of EU data protection law.

Many privacy supporters in Europe have long hoped that the US would eventually agree to harmonize its privacy laws. When the EU Data Protection Directive was adopted in 1995 and implemented in 1998, that was the expressed wish of EU regulators. The US Congress, however, never came close to agreeing to such a wide-ranging set of regulations on private-sector data processing. The US has more of a laissez-faire approach in this realm, while in Europe there is greater support for the "protective principle" – the government should limit certain kinds of risky activities (including processing of personal data) until it is clear that the benefits of the innovation outweigh the costs.

The EU has now adopted an update to the Directive, called the General Data Protection Regulation, which will enter into effect in 2018. Members of the European Parliament and other EU privacy supporters have once again expressed hope that the US would adopt essentially similar legislation. Meanwhile, the litigation brought by Max Schrems has challenged US surveillance practices, as applied to the personal data of EU citizens when held in the US. Supporters of the Schrems view – that the US lacks "adequate" protection – have advocated for the US adopting the fundamental rights guarantees for privacy, data protection, and redress of individual rights that are contained in Articles 7, 8, and 47 of the European Charter of Fundamental Rights of the European Union.

(2) Inter-operability. Based on my experience, there is little likelihood that the US will adopt data protection laws that have the many requirements set forth in EU law. A more likely approach is to continue to find ways to enable "inter-operability" – the ability of a company to operate in both the EU and US, subject to certain conditions.

The EU-US Safe Harbor, as agreed to in 2000, was one mechanism for inter-operability. Under the Safe Harbor, a company wishing to transfer data to the US could make a set of promises: if the company agreed to meet the requirements of the Safe Harbor, then the company had a lawful basis for transferring the data. Under this approach, there was no overall change in US law. Nor was there any in EU law, which already provided for transfers where "adequate"

safeguards existed. Instead, an individual company could enter into a binding commitment to meet the core requirements of EU law. If the company made this commitment, then the company could share data between the two regimes.

Today, there are three principal mechanisms that enable inter-operability. First is the Privacy Shield, which is the new agreement reached in 2016 between the EU and US that has replaced the Safe Harbor. Second is use of standard contract clauses, where an entity in the EU (such as the corporate affiliate in Ireland) makes privacy promises with an entity in another country (such as the corporate affiliate in the US). Third is a company agreeing to "Binding Corporate Rules," as supervised by one of the EU data protection authorities.[2]

(3) Potential conflicts between regimes. Harmonization occurs when the laws of the two regimes are sufficiently similar. Inter-operability works when there are specialized measures that enable lawful data flows, under specified conditions. Sometimes, however, the conflict between the regimes is harder to resolve, and there is no acknowledged legal way to operate in both regimes.

One possibility is that the "stricter" regime will cause consequences for the other regime. This would happen, for instance, if the European Court of Justice strikes down standard contract clauses and Privacy Shield, based on the view that the US lacks sufficient safeguards against surveillance. My own view is that the US safeguards are stronger than the corresponding EU safeguards, but that issue is now before the courts in the EU. If the EU makes such a holding, then it may become illegal in many circumstances to send personal data from the EU to other countries.

Another possibility is that one regime is stricter on the face of the law, but does not enforce that strict standard. One often-made observation is that the EU may have stricter privacy laws on the books, but "privacy on the ground" is considerably less strict there. Privacy laws in some instances are aspirational – what the legislators announce should be good practice – but in practice do not require strict compliance. One example may be the prohibition in the Data Protection Directive against making decisions "based solely on automated processing of data." In practice, online web sites make innumerable decisions based on automated processing of data, including about which advertisements and products to show to the user. Limits on such decisions may become more strictly enforced under the General Data Protection Regulation, which goes into effect in 2018. To date, however, the prohibition on automated decisions has been strong in theory but almost never enforced in practice. In light of the lack of enforcement, companies have had the ability in practice to operate similarly on both sides of the Atlantic.

[2] The potential importance of the case brought by Max Schrems is that none of these three mechanisms can limit the actions of the US government to use legal process within the US to access personal data. If the US government surveillance access violates EU law, then it is possible that none of these inter-operability mechanisms will enable data flows from the EU to the US.

(C) Resources for further reading. Here are some additional readings that address these issues of harmonization and inter-operability for EU/US data flows, alphabetically by author:

Tiffany Curtiss, Privacy Harmonization and The Developing World: The Impact Of The EU's General Data Protection Regulation On Developing Economies, 12 Wash. J. L. Tech. & Arts 95 (2016).

"The General Data Protection Regulation can be an ideal model for global harmonization of privacy laws, particularly for adoption among industries and willing participants. To benefit from a co-regulatory approach, however, a developing economy would need to invest in education and legal systems in order to capture the benefits of the growing e-commerce market that will undoubtedly be influenced by the General Data Protection Regulation."

Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 Stan. L. Rev. 1315 (2000).

"Professor Reidenberg postulates that harmonization of the specific rules for the treatment of personal information will be harmful for the political balance adopted in any country and offers, instead, a conceptual framework for coregulation of information privacy that can avoid confrontations over governance choices. The theory articulates roles for institutional players, technical codes, stakeholder summits and eventually a treaty level "General Agreement on Information Privacy" to develop mutually acceptable implementations of the universally accepted core principles."

Paul M. Schwartz, The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures, 126 Harv. L. Rev. 1966 (2013).

"This Article argues that this policymaking has not been led exclusively by the EU, but has been a collaborative effort marked by accommodation and compromise…The Article then analyzes the likely impact of the Proposed Regulation, which is slated to replace the Directive. The Proposed Regulation threatens to destabilize the current privacy policy equilibrium and prevent the kind of decentralized global policymaking that has occurred in the past."

Scott J. Shackelford & Andraz Kastelic, Toward A State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity, 18 N.Y.U. J. Legis. & Pub. Pol'y 895 (2015).

"This Article analyzes thirty-four national cybersecurity strategies as a vehicle to discover governance trends that could give rise to customary international law norms across the dimensions of critical infrastructure protection, cybercrime mitigation, and governance."

Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1 (2000).

Describing how stricter EU privacy standards have ratcheted up U.S. privacy standards by both legal and social means, for example, by encouraging self-regulation by U.S. businesses or providing a benchmark for civil society groups.

Gregory Shaffer, Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements, 9 Colum. J. Eur. L. 29 (2002).

"The Article concludes that, overall, transatlantic institutional adaptation has been slow (and often creeping), but where it has occurred, it largely has been along EC, and not U.S., models. The United States has adopted international standards that mirror those of the EC, delegated testing and product assessment responsibilities to private bodies reflecting an EC "global" regulatory approach, and coordinated the oversight of these bodies under a new U.S. national program analogous to those operating in the EC for over a decade. The United States has done so because of the EC's growing market clout and because the EC offers a model that actually works in combining regulatory diversity with high levels of economic exchange."

Peter Swire, Elephants and Mice Revisited: Law and Choice of Law on the Internet, 153 U. Pa. L. Rev. 1975 (2005).

Examines the evolution of choice of law with respect to cyberlaw issues, including privacy and cybersecurity.

Peter Swire & DeBrae Kennedy-Mayo, How Both the EU and the U.S. Are 'Stricter' Than Each Other for the Privacy of Government Requests for Information, 66 Emory L.J. (forthcoming 2017), available at https://ssrn.com/abstract=2920748.

This Article compares the relative strictness in the law enforcement context of EU and US legal protections, and explains implications for current legal debates about the "adequacy" of US protections under EU laws. It also analyzes possible paths to improve inter-operability for Mutual Legal Asssitance requests.