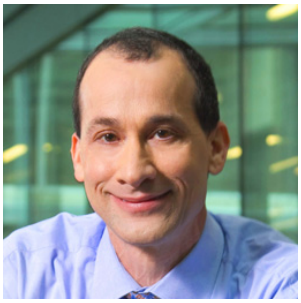
MyIAPP

Differing Privacy Regimes: A Mini-Poll on Mutual EU-U.S. Distrust



By Paul Schwartz

Privacy Perspectives | Jul 22, 2014

There are notable differences between EU and U.S. data protection law. There is also equally notable skepticism in the U.S. and EU about the other legal system's approach

To help illustrate the nature of these doubts, I contacted a handful of leading U.S. privacy attorneys to gather their opinions of EU data protection law. Then, to round out this mini-poll, I asked privacy attorneys in Germany during a recent visit to Cologne and Frankfurt-am-Main about their views of the U.S. system of information privacy law. All were promised confidentiality; data protection is, after all, an important matter.

Here are the views of the U.S. attorneys regarding EU privacy law:

- The EU approach to privacy is long on process and short on substance. Where it is substantive, it seems blind to the places where EU privacy directives and other EU regulatory measures are inconsistent with non-privacy EU directives.

- The EU approach is not actually enforced. It is law on the books plus rhetoric by regulators that extends the law even further. But the law is only occasionally enforced. As a result, much activity exists in a gray zone of risk.

- American legal culture is more literal and more compliance-minded than Europe's. In the EU, there is an aspirational, hortatory, vague legal regime, which would literally make the entire Internet "illegal." Americans simply cannot translate such aspirational principles into their own more literal and more litigious system.

- EU regulators often seem to believe that most data use is about marketing. But a wide range of data use is focused on adding value to society. Benefits to users or to society are often minimized as a basis for processing.

- Some in the EU recoil at the mention of innovation made possible through the use of personal data, almost making mention of it off-limits.

- Some in the EU *still* think that national security surveillance is a U.S. problem alone and that EU clouds will solve that problem.

As these points illustrate, the U.S. concerns about EU data protection are deep. They are matched, however, by the EU distrust of U.S. information privacy law.

Here are the views of the German privacy experts:

- U.S. law has a limited concept of privacy harms. Without a concept of "personality rights" to anchor information privacy law or some equally effective principle, many privacy harms to persons are not addressed by U.S. law.

- There is no obligation of the state in the U.S. to take active measures to protect individual privacy. In German law, there is a strong such requirement—the notion is that of a protective duty ("*Schutzpflicht*").
- In the absence of an omnibus privacy law in the U.S., there is a confusing multiplicity of laws, federal and state. This multiplicity leads to a "fragmentation of the legal field" ("*Zersplitterung des Rechtgebiets*").

- The Snowden revelations and other information about the NSA's activities reveal shameless behavior by the U.S. For example, *Der Spiegel* has revealed that the U.S. had monitoring equipment installed within its Berlin embassy.

- The NSA is acting to make cybersecurity weaker. This behavior endangers a shared interest in strong security.

- The NSA is carrying out industrial espionage on behalf of U.S. companies.

- U.S. companies have strong market dominance in IT, and the result is arrogant behavior.

- EU policy-makers feel overwhelmed by the sheer volume of the lobbying efforts by U.S. companies

Many of these comments from the German experts reflect fundamental differences in how the U.S. regulates privacy law, which leaves experts on the European side of the Atlantic feeling that the American system does not contain effective protections.

The comments also show a profound and continuing reaction to the Snowden revelations. One year after the "Summer of Snowden," that is, the initial release of NSA documents by Edward Snowden, emotions are still running high in Germany about U.S. global surveillance activities. Indeed, outside the campus of the Goethe University Frankfurt, I passed pro-Snowden posters stuck on telephone poles. The posters featured a simple suggestion for Germany's policy in this matter: "Asyl," that is, an offer of asylum in Germany for Snowden.

Many of these comments from the German experts reflect fundamental differences in how the U.S. regulates privacy law, which leaves experts on the European side of the Atlantic feeling that the American system does not contain effective protections.

Moreover, Chancellor Angela Merkel herself was said to be upset by the report that the U.S. had spied on her cell phone. As one attorney told me in Cologne, "Allied nations should not behave this way with each other." It should be noted that this anger continues—the latest flare-ups are due to recent German media revelations of an American spy within the *Bundesnachrichtendienst*, Germany's foreign intelligence agency. In response, Germany has expelled the CIA's top officer in Berlin.

The fallout from the Snowden leaks is also having significant business implications for U.S. technology firms. In June, the German government announced it would end a contract with Verizon Communications because of concerns about network security. It is shifting its business to Deutsche Telekom, a German company. Microsoft General Counsel Brad Smith also stated recently that the business issues relating to the Snowden links were "getting worse, not better." Forrester Research has estimated that the NSA disclosures could reduce U.S. technology sales overseas by as much as $180 billion by 2016.

There are no easy solutions to differences in EU-U.S. data protection. Instead, there are only tough discussions ahead. There are, however, two lessons that can be drawn from my mini-survey.

First, the U.S. attempt to launch a discussion around the term "interoperability" is unlikely to be fruitful. In the White House's 2012 "Report on Consumer Data Privacy in a Networked World,"

the executive branch declared its "commitment to increase interoperability with the privacy frameworks of our international partners." The plan was a good one. The U.S. privacy system is not like that of the EU, and its goal should not be to become the equivalent of it.

The overarching idea of "interoperability" is to allow different privacy systems to work together. It is hard to object to that idea in the abstract, and the OECD's 2013 Privacy Guidelines call for greater efforts to address the global aspects of privacy through improved interoperability. Due to current high levels of suspicion on the EU side, however, the idea of "interoperability" now has the air of "Pax Americana," or an agreement enforced on the world through American power. I have yet to meet a single privacy policy-maker in Europe who reacted favorably to this term. It is probably time to drop that "brand." Nonetheless, the policy goals of the 2012 White House report regarding accountability and enforcement are highly valuable. A discussion around these concepts has the potential to discover new common ground.

Due to current high levels of suspicion on the EU side, however, the idea of "interoperability" now has the air of "Pax Americana," or an agreement enforced on the world through American power. I have yet to meet a single privacy policy-maker in Europe who reacted favorably to this term.

Second, "harmonization networks" for information privacy are more important than ever before. "Harmonization networks" develop when regulators and other policy-makers in different countries work together to harmonize or otherwise adjust different kinds of domestic law to achieve outcomes favorable to all parties. This general phenomenon was first noted by the international law scholar Anne Marie-Slaughter. As Slaughter writes, "The more that international commitments require the harmonization or other adjustment of domestic law, the coordination of domestic policy or cooperation in domestic enforcement efforts, the more they will require government networks to make them work."

An important way forward will be through further policy engagement and discussions among the informal networks of government officials and policy-makers concerned with international privacy law. One promising locus for these efforts is the Global Privacy Enforcement Network, of which the U.S. Federal Trade Commission is a founding member. Increased global collaboration in privacy investigations and enforcement actions worldwide will help develop shared goals of accountability and enforcement. It may also help defuse at least some of the current distrust and tensions between the EU and U.S. about information privacy law.

Written By

Paul Schwartz

Paul Schwartz is a leading international expert on information privacy law. He is a professor at the University of California, Berkeley Law School and a director of the Berkeley Center for Law and Technology. He has testified before Congress and served as an advisor to international organizations, including Directorate Generals of the European Union. He assists numerous corporations and organizations with regulatory, policy and governance issues relating to information privacy. Schwartz is a frequent speaker at technology conferences and corporate

events in the United States and abroad. He is a Special Advisor to the privacy and data security practice of Paul Hastings LLP.

Professor Schwarz is the author of many books, including the leading casebook, "Information Privacy Law," and the distilled guide, "Privacy Law Fundamentals," each with Daniel Solove. "Information Privacy Law," now in its fourth edition, is used in courses at more than 20 law schools. Schwartz's over fifty articles have appeared in journals such as the Harvard Law Review, Yale Law Journal, Stanford Law Review, University of Chicago Law Review and California Law Review. He publishes on a wide array of privacy and technology topics including data analytics, cloud computing, telecommunications surveillance, data security breaches, health care privacy, privacy governance, data mining, financial privacy, European data privacy law, and comparative privacy law.
www.paulschwartz.net

https://privacyassociation.org/news/a/differing-privacy-regimes-a-mini-poll-on-mutual-eu-u-s-distrust/