

How Julie Brill Is Cultivating a Defense of the U.S. Privacy Framework

[Jedidiah Bracy, CIPP/E, CIPP/US](#)

[Privacy Perspectives](#) | Feb 24, 2015



U.S. Federal Trade Commissioner Julie Brill has been busy cultivating a defense of the U.S. privacy framework while also planting seeds for lasting and meaningful interoperability with Europe. Late last year at the IAPP Data Protection Congress 2014 in Brussels, Brill sat down with the CNIL's Isabelle Falque-Pierrotin to discuss the EU-U.S. privacy divide.

Plus, late last month, she was part of [a must-see panel discussion](#) with the European Commission's Paul Nemitz. At times friendly and collegial while at others serious and contentious, the debate delved into the tricky fate of the Safe Harbor agreement, European concerns since the Snowden disclosures in 2013 and the role the Federal Trade Commission (FTC) plays enforcing that agreement.

Keep in mind, her discussion with Nemitz at CPDP wasn't long after a not-so-usual visit to the FTC from the U.S. President Barack Obama—the first visit by a U.S. president since the 1930s—and the release of a highly anticipated report on the Internet of Things (IoT). Plus, last

week, Brill spoke at Dartmouth College's Tuck School of Business on the "[Global Regulation of Data Flows in a Post-Snowden World](#)."

Her speech to one of the top business schools in the country is instructive. As she pointed out, "The Internet has become today's global trade route." And with a huge growth in economic activity over the Internet, global information flows are a huge part of sustaining many economies around the world. Key to these flows, of course, is the flow of personal data and, hence, consumers' trust. Cue the legions of privacy professionals.

Maintaining consumer trust goes beyond state or national borders, she notes. This is a global system with different data privacy and security laws, but one fraught with misunderstandings, particularly by "some international thought leaders—within the government, business community and civil society of our trading partners—who do not fully understand U.S. privacy law." *Zing!*

Brill is stalwart, but thoughtful, in her defense of the U.S. consumer privacy framework. "The notion that the United States doesn't have a privacy law stems primarily from the fact that we do not have a single, comprehensive law that governs the collection, use and disclosure of personal information in the commercial sphere," she said at Dartmouth.

In her panel discussion with the Nemitz, Brill said the U.S. system is robust, but conceded it can use improvements, specifically in beefing up student privacy protections, generating a Consumer Privacy Bill of Rights and data broker legislation. But ultimately, the "U.S. system is deeply effective," she said. Section 5 of the FTC Act allows for both robust and flexible enforcement, and, importantly, it allows the FTC to survey and target areas that need improvement. In recent months, for example, the FTC has reached settlements with a company in the IoT landscape, a Safe Harbor certification provider and the operator of a revenge porn website.

"We have a great capacity for enforcement," she said during the CPDP panel with Nemitz, and the FTC is always willing to work with other data protection authorities around the world.

Yet, the Safe Harbor agreement hangs in the balance and was a clear point of contention with Nemitz, who took issue with the FTC for not responding to European citizens' complaints about certain businesses under the Safe Harbor umbrella.

"We do not run a mediation service at the FTC," Brill explained. "We're not structured to do that. We don't do that for U.S. citizens or European citizens or Asian citizens ... Safe Harbor is no exception or different from all the other complaints we get every year." She said it's important that the FTC look more broadly and not simply depend on consumer complaints because there are many nonconsumer-facing businesses that are violating people's privacy without public knowledge. In fact, in an email to me, she noted that back in the 1960s, Ralph Nader and others criticized the FTC for the exact opposite approach: Being too reliant on consumer complaints, which, previously had led the agency to miss some of the bigger issues not transparent to customers, and were therefore not the subject of consumer complaints.

Really, the FTC can be selective and react to issues raised by the media or other security researchers, like newly appointed FTC Chief Technologist Ashkan Soltani, who once contributed to *The Wall Street Journal's* groundbreaking "What They Know" series.

Though FTC enforcement has been robust, Brill backs the strengthening of the U.S. privacy framework. In the IoT landscape, for example, many data sets previously under the jurisdiction of sector-specific laws such as health and finance are now flowing through entities not covered by current statutes.

Additionally, Brill is adamant that nonconsumer-facing industries—so-called data brokers, most notably—be brought under consumer protection legislation. In her speech to the Tuck School of Business, she explained, “Consumers deserve much more transparency and control concerning” the profiles compiled by data brokers.

Clearly, though, global interoperability and the fate of Safe Harbor is a major issue for Brill. The Snowden revelations have injected state surveillance into the equation, with Europeans like Nemitz focusing particularly on the ability for EU citizens to have judicial redress in the U.S., but Brill maintains that it’s important to make a distinction between government surveillance and commercial collection of consumer data. And on that latter score, the FTC, she argues, is an effective enforcement backstop to Safe Harbor.

“Safe Harbor is a solution, not a problem,” she said, highlighting 24 Safe Harbor enforcement actions since 2009, and a settlement late last year with TRUSTe over its Safe Harbor certification program.

Ultimately, Brill is optimistic about resolving tensions with Europe. “Part of my optimism goes back to the common privacy principles that we share and the efforts underway on both sides of the Atlantic to examine whether our different privacy frameworks are sufficiently able to protect consumers in an era of big data and the Internet of Things.” For her, it’s not about whether the U.S. or the EU system is the “winning” system; it’s about whether both sides of the Atlantic will be able to develop an interoperable framework to keep a lucrative data-driven economy going. And one that consumers will trust.

For her part, Commissioner Brill—well, you know—she’ll continue to cultivate her defense of the U.S. privacy framework and outreach for interoperability in the hopes of a nourishing harvest for both sides of the Atlantic for years to come.

Top image taken from the [Computers, Privacy and Data Protection Conference](#) in Brussels, Belgium last January.

Editor's Note:

Commissioner Brill will take part in the Conversations in Privacy Series with Hogan Lovells Partner Christopher Wolf at next week’s [IAPP Global Privacy Summit](#) in Washington, DC.