Back to the Future: Meeting Privacy Challenges
Through a Strong Transatlantic Relationship
Forum Europe – 6th Annual Privacy and Data Protection Conference
Brussels, Belgium
December 10, 2015

Good morning. Thank you, Paul Adams, for your introduction. And thank you to Forum Europe for inviting me to speak with you this morning. Rarely have discussions about Commission's adequacy decision, which was a fundamental piece of the U.S.-EU Safe Harbor Framework. The Schrems decision came along after the United States and the European Commission had spent nearly two years negotiating terms to strengthen Safe Harbor in the wake of Edward Snowden's revelations about some of the foreign intelligence surveillance activities conducted by the United States.

I would like to spend my time with you this morning making the case for why we need to reach an agreement on a replacement for Safe Harbor, and how data protection authorities on both sides of the Atlantic can then work together to address the urgent challenges facing consumers as they navigate the increasing complex digital ecosystem.

Why We Need a General, Transparent, FTC-Enforceable Transatlantic Data Transfer Mechanism

Privacy advocates on both sides of the Atlantic celebrated the Schrems decision for its articulation of a strong right to privacy in Europe. And the decision is helpful in this regard. It crystallized what has been clear – or should have been clear – for a long time about commercial privacy in Europe: it is a fundamental right that Europeans and the Court take very seriously.

But consumers and companies on both sides of the Atlantic lost something important with the Schrems decision. The first loss is transparency. When a company joined Safe Harbor, consumers knew it, advocates knew it, and the entire enforcement community knew it. The principles and operating procedures for Safe Harbor were also well known and uniform.

[2] The same cannot be said for other data transfer mechanisms, such as binding corporate rules and model contractual clauses. With respect to model contract clauses, some data protection authorities might require companies to file copies of their model contracts, but that is not the

[1] Schrems v. Data Protection Comm'r, CJEU Case C-362/14 (Oct. 6, 2015), available at http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=.

[2] See Dept. of Commerce, U.S.-EU Safe Harbor List, Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, http://export.gov/safeharbor (last visited Dec. 9, 2015).

case with every data protection authority.[3] And although companies with approved binding corporate rules are listed on the European Commission's website,[4] the details of the rules that each company creates for itself are not public. As a result, neither of these arrangements provides anywhere near the level of transparency that Safe Harbor provided.

The second loss is FTC enforcement. Simply put, the absence of Safe Harbor may limit the FTC's ability to take action against companies if they misrepresent how they follow European privacy standards. And, in the absence of Safe Harbor, there is little reason for companies to make those representations in the first place.

Ironically, among Safe Harbor companies it is small and medium enterprises that stand to

comparison of the United States' laws (or the laws of any third country) to European legal ideals as enshrined in the Charter of Fundamental Rights. Whether the ECJ agrees with me remains to be seen. But, in the meantime, I would like to discuss the many ways that the United States protects personal data. Our framework is a combination of constitutional, statutory, and administrative protections. This makes it maddeningly difficult to explain to people who don't spend every day immersed in its details. But it's important to know those details, because they are integral to the honest conversation about privacy that needs to take place between Europe and the U.S.

Where the government's

conditions,[16] and requiring online services to allow minors to delete information they have posted[17] – to requiring companies to notify consumers when they suffer a security breach involving personal information.[18]

For the past two decades, consumer privacy has been one of the top priorities at my agency, the U.S. Federal Trade Commission. We enforce many of the federal laws aimed at protecting sensitive information that I just mentioned. We also use the FTC Act, which prohibits "unfair and deceptive practices" to address privacy and data security in many of the commercial areas that are not subject to these sector-specific laws. Under this authority, we have taken aim at a broad array of privacy harms. For example, we have brought actions against companies for allegedly collecting information inappropriately from consumers' mobile devices,[19] making unwarranted intrusions into private spaces,[20] exposing health and other sensitive information, exposing previously confidential information about individuals' networks of friends and acquaintances,[21] and providing sensitive information to third parties who in turn victimize consumers.[22]

The FTC's enforcement expertise gave teeth to our ability to ensure that companies lived up to their Safe Harbor commitments. We had brought 39 actions against companies for misrepresenting that they were members of the Safe Harbor or misrepresenting that they complied with the Safe Harbor principles. Among these actions were our settlements with Google[23] and

---

passwords-2013.aspx (last updated Nov. 18, 2014) (noting that in 2014, at least 28 states had introduced social media and employment legislation or had such legislation pending).

[16] See, e.g., Privacy Rights Clearinghouse, California Medical Privacy Fact Sheet C5: Employment and Your Medical Privacy, available at https://www.privacyrights.org/content/employment-and-your-medical-privacy (last updated July 2012).

[17] See CAL. BUS. & PROFS CODE § 22580 et seq., available at http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22580

[18] See Nat'l Conf. of State Legislatures, Security Breach Notification Laws (Jan. 12, 2015), available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (collecting references to over 45 state laws).

[19] See, e.g., Goldenshores Techs. LLC C-4466 (F.T.C. Mar. 31, 2014) (decision and order), available at https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.

[20] See FTC, Press Release, Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees (Oct. 22, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer

[21] See Facebook, Inc., C-4365 (F.T.C. July 27, 2012) (decision and order), available at https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf/

[22] FTC v. Sitesearch Corp., d/b/a LeapLab (D. Az. Dec. 23, 2014) (complaint), available at http://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf

[23] Google, Inc., C-4336 (F.T.C. Oct. 13, 2011) (decision and order), available at https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

Facebook,[24] in which we alleged that those companies had violated their substantive commitments under Safe Harbor. All of our Safe Harbor enforcement actions entailed placing the companies under twenty-year orders that prohibit them from making such misrepresentations in the future. Hundreds of millions of EU citizens are protected under these orders. Moreover, because we were receiving very, very few referrals from European DPAs regarding Safe Harbor violations, we decided to examine, in each of our domestic privacy and data security investigations, whether the company in question is a member of Safe Harbor, and whether its activities may have violated the Safe Harbor principles. Finally, the FTC has the authority to share confidential information with our international law enforcement partners, and we have a lot of experience working with them on investigations. The FTC is ready to use these same tools to enforce the enhanced protections that I believe will be built into Safe Harbor's replacement.

* * * * *

Once we have a new data transfer mechanism in place, and once we begin to have an honest conversation about the ways in which law enforcement and intelligence data collection practices may be essentially equivalent, then the United States and Europe will be in a position to face the future challenges that the Internet of Things and big data analytics present for privacy and data protection. I believe it is in the

Commissioners have called for Congress to enact more robust consumer privacy laws, because we concluded that they would create more effective protections for U.S. consumers in this highly connected, data intensive world.[38] For example, I have called for baseline privacy legislation to fill the growing gaps in protection of sensitive information that now flows outside the decades-old silos of our laws protecting financial, health and credit reporting data.[39] I have also been a strong advocate of data broker legislation that would provide much needed transparency, access and correction rights to the consumer profiles that are created and sold by data brokers.[40] And the FTC has pressed Congress to enact federal data security legislation.[41] But let me be absolutely clear: although I support additional consumer privacy legislation in the U.S., I do not believe such legislation is prerequisite for a post-Schrems data transfer mechanism. The case for enacting these laws was compelling before October 6th. After a more durable data transfer mechanism is in place to allow more seamless data flows between the U.S. and EU, the Schrems decision may, in the longer term, help restart efforts in the United States to put in place stronger privacy and data security laws that will benefit all.

Currently, the EU, U.S., and other regions face common benefits and challenges from big data and connected devices. Well before the ECJ issued its watershed Schrems decision, we at the FTC had been working with our counterparts in Europe to identify specific challenges and focus on the common principles that would apply to these technologies. The Schrems decision does not take away that common ground, nor does it diminish the importance of working together to understand the privacy implications of new technologies, cooperating on enforcement matters when possible, and bringing our own actions when warranted.

* * * * *

The Schrems decision has grabbed the attention of American stakeholders, many of whom see the need to have an honest conversation about the strengths and weaknesses of privacy protections on both sides of the Atlantic. I hope the decision will also motivate European stakeholders to join us in that honest discussion.

Thank you.

---

[38] See FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS i (2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[39] See, e.g., Julie Brill, Commissioner, A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data, at 9 (Oct. 23, 2013), available at https://www.ftc.gov/public-statements/2013/10/call-arms-role-technologists-protecting-privacy-age-big-data

[40] See Julie Brill, Commissioner, Statement on the Commission's Data Broker Report (May 27, 2014), available at https://www.ftc.gov/public-statements/2014/05/statement-commissioner-brill-commissions-data-broker-report

[41] See