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 Adamson, for your introduction. And thank you to Forum Europe for inviting me to speak with you this morning. Rarely have discussions about the challenges surrounding the data-driven economy, privacy, and values in democratic societies been more urgent, and Brussels is at the center of many of those discussions.

It has been about two months since the European Court of Justice (ECJ) shook the data protection world with its decision in *Schrems v. Data Protection Commissioner*.[1] That decision, as many of you know, invalidated the European 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 their 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 lose the most from the *Schrems* decision. Although some of the companies that joined Safe Harbor are the globally recognized giants of the Internet economy, many were not. Around 60 percent of Safe Harbor companies were small and medium enterprises (SMEs).[5] Like the biggest companies, these SMEs depend on the free flow of information to sell goods and services globally, build global workforces, and take advantage of low-cost cloud computing resources. Unlike the big companies, however, these SMEs do not have the time or resources to get BCRs approved or put model contractual clauses in place.

The ECJ's decision in *Schrems* focused on two deficiencies in the European Commission's original decision in 2000 regarding Safe Harbor: first, the Court worried about the Commission's silence on existing safeguards in the U.S. with respect to government access to personal data for purposes of national security surveillance;[6] and second, the Court was concerned about the lack of any information about the availability of redress for individuals with respect to government access to personal data. The Court further held that, before there can be a finding of "adequacy" of the laws of another country or a data transfer mechanism, the European Commission must demonstrate tht the privacy laws and other protections are "essentially equivalent" to those found in the European legal order.

I believe that this "essentially equivalent" standard requires a comparison between laws as they actually exist in the United States and at the EU and Member State levels, rather than a

---

[3] *See, e.g.*, Data Protection Commissioner of Ireland, Model Contracts: Approved Arrangements for Transferring Data to Third Countries, *available at* https://www.dataprotection.ie/docs/Model-Contracts/38.htm (stating that Ireland does not require Irish data controllers to deposit contracts with non-EEA data processors or data controllers) (last visited Oct. 15, 2015).

[4] *See* European Commission, List of Companies for Which the EU BCR Procedure Is Closed (last updated Sept. 13, 2015), *available at* http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

[5] *See* U.S. Dept. of Commerce – Int'l Trade Admin., Key Points Concerning the Benefits, Oversight, and Enforcement of Safe Harbor, *available at* https://build.export.gov/build/idcplg?IdcService=DOWNLOAD_PUBLIC_FILE&RevisionSelectionMethod=Latest&dDocName=eg_main_092414 (last visited Dec. 9, 2015).

[6] *See Schrems*, *supra* note 1, at ¶¶ 89-91.

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* collection of personal data is concerned the idea of a fundamental right to privacy is very much a part of the U.S. legal fabric. The U.S. Constitution provides fundamental protections for individual privacy rights by limiting government searches and seizures;[7] and the U.S. Supreme Court and other federal courts have in recent years extended these rights to new technologies and new forms of communication.[8] Laws passed by Congress set additional limits on law enforcement access[9] and intelligence surveillance.[10]

Turning to the commercial sphere, the U.S. privacy framework includes important laws that are designed to protect sensitive information about children,[11] financial information,[12] medical data,[13] and information used to make decisions about consumers' credit, insurance, employment and housing.[14] In addition, the states have many additional commercial privacy laws that range from limiting employers' ability to view their employees social network accounts,[15] prohibiting employers and insurers from using information about certain medical

[7] *See* U.S. Const. amend. IV, *available at* https://www.law.cornell.edu/constitution/fourth_amendment.

[8] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that the search of an arrestee's cell phone generally requires a warrant); United States v. Jones, 565 U. S. ___ 132 S. Ct. 945 (2012). See also United States v. Warshak 631 F.3d 266 (6th Cir. 2010). In addition, in the past two years the United States has taken executive action and enacted legislation that limit foreign intelligence surveillance practices. *See, e.g.*, USA FREEDOM Act, Pub. L. 114-23, *available at* https://www.congress.gov/bill/114th-congress/house-bill/2048/text?q=%7B%22search%22%3A%5B%22%5C%22hr2048%5C%22%22%5D%7D&resultIndex=1&overview=closed; Presidential Policy Directive – Signals Intelligence Activities (PPD-28) (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[9] *See, e.g.*, Wiretap Act (codified as amended at 18 U.S.C. §§ 2510-22) and Electronic Communications Privacy Act (codified at 18 U.S.C. §§ 2701-12).

[10] See, e.g., Foreign Intelligence Surveillance Act, (FISA) 50 U.S.C. § 1801 *et seq.* FISA was recently amended through the USA FREEDOM Act, *supra* note 8.

[11] *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06.

[12] 15 U.S.C. §§ 6801-09.

[13] Health Insurance Portability and Accountability Act, Pub. L. No.104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

[14] 15 U.S.C. § 1681 *et seq.*

[15] *See* Nat'l Conf. of State Legislatures, Employer Access to Social Media Usernames and Passwords, *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-

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 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/systems/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.

Addressing the Challenges Beyond *Schrems* and Safe Harbor

Now let me turn to the challenges that lie beyond Safe Harbor. I urge us all to consider implementation of a more robust, durable successor to Safe Harbor to be the beginning, not the end, of a renewed effort to work together across the Atlantic on strengthening privacy protections. I believe the ECJ's decision in *Schrems* adds to the growing body of evidence that there is a need for a shift in the way that we – on both sides of the Atlantic – have framed privacy. In the U.S., we have largely separated the discussions about data practices of commercial firms from the data practices of the government. Within this framework, the FTC carries out its commercial privacy enforcement program as a purely civil law enforcement agency. As a result, the interests of consumers simply have not been directly implicated by the debates that have surrounded criminal law enforcement investigations.

That is, until recently. In the United States, there is a growing debate over whether to enact legislation that requires companies to have a means to provide law enforcement with access to unencrypted versions of encrypted communications in response to a court order or warrant. This debate has started to chip away at the silos around consumer interests in commercial privacy and citizens' interest in protection from unwarranted intrusion by government. Some law enforcement agencies have drawn attention to the barriers that encryption presents when the keys are controlled by consumers, who are sometimes the targets of their investigation.[25] Many security experts and privacy advocates argue, however, that any other plausible arrangement would introduce vulnerabilities into devices and networks that would put consumers' data and devices at an unacceptable risk.[26] I have come down on the side

[24] *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/.

[25] *See* Statement of Sally Quillian Yates, Deputy Attorney General, Department of Justice, and James B. Comey, Director, Federal Bureau of Investigation, Before the Senate Judiciary Committee Hearing on Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy (July 8, 2015), *available at* http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Yates%20and%20Comey%20Joint%20Testimony1.pdf.

[26] *See, e.g.*, Harold Abelson et al., *Keys Under Doormats*, 58 COMM. ACM 24 (Sept. 2015).

of these security experts and privacy advocates, and have worried about the "magical thinking" that appeared to lead some to believe that "back doors" could be created for law enforcement but not exploited by others in a manner that would harm consumers.[27] This debate over law enforcement's encryption challenges is likely to continue. My hope and expectation is that this debate will take into full account consumers' privacy and data security interests, and concerns about the security of our infrastructure.

Consumers' interests in commercial privacy and citizens' interest in protection from governmental intrusion also collided when the FTC was asked to testify on legislation to revise the authority of law enforcement agencies to obtain the contents of communications from email providers, social networks, cloud services, and other service providers.[28] Some reform proposals to modernize this law and further restrict law enforcement access have broad support in Congress.[29] These proposals would essentially prohibit civil law enforcement agencies like the FTC from going to service providers to obtain communications content during their investigations[30] – something that the civil agencies can do now, but only in limited circumstances. I took the view that the FTC has not in fact used this authority, it doesn't not need this authority, and that allowing civil law enforcement agencies to use such authority raises significant consumer privacy and constitutional concerns.[31]

As these examples illustrate, in the United States, we are engaged in a robust conversation about these issues. Many of the same issues are now on the table in Europe. I believe European policymakers and stakeholders should engage in this discussion as well, and examine their Member States' own law enforcement and intelligence data collection practices with the same openness and recognition of the potential impact the practices may have on consumers' and citizens' privacy.

---

[27] *See* Editorial, Putting the digital keys to unlock data out of reach of authorities. WASH. POST (July 18, 2015), *available at* https://www.washingtonpost.com/opinions/putting-the-digital-keys-to-unlock-data-out-of-reach-of-authorities/2015/07/18/d6aa7970-2beb-11e5-a250-42bd812efc09_story.html (reaffirming a call for technology companies to create "a kind of secure golden key that could unlock encrypted devices, under a court order, when needed").

[28] *See* Senate Judiciary Committee, Reforming the Electronic Communications Privacy Act (Sept. 16, 2015), http://www.judiciary.senate.gov/meetings/reforming-the-electronic-communications-privacy-act.

[29] *See* Email Privacy Act, H.R. 699 (Feb. 4, 2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/699 (listing 301 cosponsors).

[30] *See* H.R. 699, *supra* note 29; Electronic Communications Privacy Act Amendment Act, S. 356, *available at* https://www.congress.gov/bill/114th-congress/senate-bill/356/related-bills (last visited Oct. 22, 2015).

[31] *See* Julie Brill, Statement About the Federal Trade Commission's Written Testimony on "Reforming the Electronic Communications Privacy Act Submitted to Senate Judiciary Committee" (Sept. 16, 2015), *available at* https://www.ftc.gov/public-statements/2015/09/statement-about-federal-trade-commissions-written-testimony-reforming.

* * * * *

Once we have a new data transfer mechanism in place, and once we begin to have an honest conversation about the ways in which our 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 these larger issues presented by newer data intensive technologies, and the highly connected world that they create, that the United States and Europe may be able to forge a constructive dialogue about common approaches – approaches that both ensure the tantalizing – perhaps even world-changing – benefits, and at the same time address the challenges these technologies pose to fundamental aspects of consumer privacy, security, and fairness in our societies.

The FTC is starting to address these challenges now. We have held public workshops where researchers, businesses, and advocates have helped us understand both the technical details and policy implications of analytics,[32] algorithms,[33] connected devices,[34] and cross-device tracking.[35] We have created the position of a chief technologist, and we are building an office filled with staff level technologists who can work along side FTC staff and Commissioners to analyze technical systems and give an independent view of the data the systems collect and how the data are used. And while we have developed best practices for businesses that are creating connected devices and other new technologies,[36] we have also brought enforcement actions against companies that fail to take reasonable steps to protect sensitive data that flow from these devices,[37] or collect or use the data in ways that defy consumers' expectations or harm them. Along with our comprehensive program of policy development and business and consumer education, our enforcement program provides a way to ensure that companies take seriously their privacy and data security obligations as they develop these new technologies.

And make no mistake: although I believe the U.S. consumer privacy framework is strong and multifaceted, I also believe the U.S. needs to go further with its consumer privacy laws to ensure that they keep up with these new technologies. For several years, I and my fellow

---

[32] *See* FTC, Spring Privacy Series: Alternative Scoring Products (Mar. 19, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.

[33] *See* FTC, Big Data: A Tool for Inclusion or Exclusion? (Sept. 15, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[34] FTC, Internet of Things - Privacy and Security in a Connected World (Nov. 19, 2013), *available at* https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[35] [Cite to cross-device tracking workshop website.]

[36] *See generally* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015) (staff report), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing views of workshop participants).

[37] *See* TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

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 we 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* FTC, Press Release, FTC Testifies on Proposed Data Security Legislation Before House Energy and Commerce Committee's Commerce, Manufacturing and Trade Subcommittee (Mar. 18, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/03/ftc-testifies-proposed-data-security-legislation-house-energy (highlighting the Commission's support for data security legislation).