Transatlantic Privacy After *Schrems*: Time for An Honest Conversation

Keynote Address at the Amsterdam Privacy Conference
Commissioner Julie Brill
October 23, 2015

Good afternoon. It is a pleasure to be in Amsterdam to discuss privacy at this momentous time. I am grateful to Nico Van Eijk for inviting me to address the conference, and I am looking forward to the many conversations that will take place on the stage and off to the sides during the next few days.

When Nico invited me three months ago, he asked me to speak to you about the Internet of Things. The rapid advance of network connections to automobiles, household appliances, clothing, and other everyday objects to create an "Internet of Things" could provide some enormous benefits to individuals and society, from allowing cities to better maintain their infrastructures to developing effective treatments to some of the most intractable diseases.[1] The Internet of Things also presents some difficult challenges to individual privacy, data security, and even physical safety. Connected devices are multiplying by the billions every year.[2] The data from these sensors – much of which will be deeply sensitive – already scale beyond most individuals' imagination, and are expected to double every year. And at the same time, the "internet will disappear", as Google's Chairman, Eric Schmidt, predicts.[3] Connectivity will just be a part of how things work, as electricity is today. This means that user interfaces will shrink or disappear, making it more challenging to ensure that consumers know when their data is being collected, or to exercise appropriate control. Figuring out ways to protect data in this highly complex, decentralized environment, as well as providing individuals with meaningful control over their information, are among the top consumer protection priorities at my agency, the U.S. Federal Trade Commission (FTC).[4]

Nico also asked me to talk about the privacy framework for commercial data in the United States, and in particular the relationship between consumer protection – a core FTC mission – and data protection in the United States. This outlook differs from the European

---

[1] *See* Julie Brill, Commissioner, Navigating the "Trackless Ocean": Privacy and Fairness in Big Data Research and Decision Making, at 1-2 (Apr. 1, 2015), *available at* https://www.ftc.gov/public-statements/2015/04/navigating-trackless-ocean-privacy-fairness-big-data-research-decision.

[2] *See* DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (predicting 25 billion connected devices in 2015 and 50 billion by 2020).

[3] *See* Chris Matyszczyck, *The Internet Will Vanish, Says Google's Eric Schmidt*, CNET (Jan. 22, 2015, 6:00 PM), *available at* http://www.cnet.com/news/the-internet-will-vanish-says-googles-schmidt/.

[4] *See* Julie Brill, Commissioner, Bitkom Privacy Conference Keynote Address, at 5-7 (Sept. 24, 2015), *available at* https://www.ftc.gov/public-statements/2015/09/keynote-address-bitkom-privacy-conference (discussing the challenges that complexity creates for security).

privacy framework, which rests on fundamental rights in the Charter,[5] the EU-wide protections in the 1995 Data Protection Directive,[6] and Member State legislation.

Privacy protection in the United States is more of a hybrid. Most of you are deeply familiar with the constitutional rights against unwarranted government intrusion,[7] as well as statutory requirements involving law enforcement access[8] and intelligence surveillance,[9] in the United States. You may be less familiar with the many specific U.S. privacy laws designed to protect information about children,[10] financial information,[11] medical data,[12] and information used to make decisions about consumers' credit, insurance, employment and housing.[13] Layered on top of these specific laws involving commercial information – and filling many of the gaps among them – is the FTC's authority to enforce our broad and remedial statute that prohibits "unfair or deceptive acts or practices in or affecting commerce."[14] In addition, the states have many additional 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 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]

---

[5] Charter of Fundamental Rights of the European Union, 2012/C 326/02 (Oct. 26, 2012), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal data and on the Free Movement of Such Data, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

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

[8] *See, e.g.*, 18 U.S.C. §§ 2510-22, 2701-12.

[9] See, e.g., 50 U.S.C. § 1801 *et seq.*

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

[11] 15 U.S.C. §§ 6801-09.

[12] 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.).

[13] 15 U.S.C. § 1681 *et seq.*

[14] 15 U.S.C. § 45(a).

[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-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).

The FTC generally targets practices that cause harm to consumers. But we have a broad notion of harm. It includes financial harm, for sure, but it also includes inappropriate collection of information on consumers' mobile devices,[19] unwarranted intrusions into private spaces,[20] the exposure of health and other sensitive information, the exposure of 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 has taken action against some of the biggest names on the Internet, including Google[23] and Facebook,[24] as well as many smaller players, for deceiving consumers about their data practices or using consumers' data in an unfair manner. And we focus on emerging new technologies – such as user generated health information,[25] facial recognition technology,[26] cross device tracking,[27] retail mobile location tracking,[28] and mobile payments[29] – to help ensure they are developed in a manner that will not harm consumers. We have obtained millions of dollars in penalties and restitution in our privacy and data security cases, such as a $22.5 million fine against Google[30] and an $11 million for

[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.

[24] *See supra* note 21.

[25] FTC, Press Release, Spring Privacy Series: Consumer Generated and Controlled Health Data (May 7, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.

[26] *See* FTC, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (staff report) (Oct. 2012), *available at* https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies.

[27] FTC, Press Release, Cross-Device Tracking, *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking (last visited Oct. 22, 2015).

[28] FTC, Press Release, Spring Privacy Series: Mobile Device Tracking (Feb. 19, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.

[29] *See* FTC, What's the Deal? A Federal Trade Commission Study on Mobile Shopping Apps (staff report) (Aug. 2014), *available at* https://www.ftc.gov/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014; FTC, Paper, Plastic . . . . or Mobile? An FTC Workshop on Mobile Payments (staff report) (Mar. 2013), *available at* https://www.ftc.gov/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments.

[30] FTC, Press Release, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

consumer redress from LifeLock.[31] And we have placed numerous companies under 20-year orders with robust injunctive provisions relating to their privacy and data security practices.

When these different parts of the U.S. privacy framework are put together, the result is a system that is strong and comprehensive. But it is also maddeningly difficult to explain to my European colleagues.

All of this – the Internet of Things and the consumer protection roots of commercial privacy enforcement in the U.S. – is deeply interesting and should be part of the rich discussion here in Amsterdam. But in light of recent events, I also need to focus on the European Court of Justice decision[32] that Max Schrems just discussed from his perspective as the plaintiff.

The European Court of Justice's Decision's Reverberations on Both Sides of the Atlantic

First, allow me to set the scene a bit on both sides of the Atlantic. As most of you know quite well, throughout Europe and in some quarters of the United States, the *Schrems* decision has been hailed as strong vindication of Europeans' fundamental right of privacy. The European Commission,[33] the data protection authorities,[34] and privacy advocates[35] have all embraced the ruling, and in different ways are laying the groundwork for moving forward to implement the requirements and principles laid out by the Court. More globally, in just two days, the data protection and privacy commissioners from around the world will gather here in Amsterdam for our annual meeting.[36] The very timely theme of the meeting will be "privacy bridges" – that is, the practical steps that enforcers and regulators can take to work together effectively, despite differences in their authority and in the laws that they enforce. Meanwhile, across the Atlantic,

---

[31] FTC, Press Release, LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False (Mar. 9, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states (stating that LifeLock agreed to pay $11 million to the FTC and $1 million to a group of 35 state attorneys general).

[32] 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=.

[33] *See* European Commission, Statement, First Vice-President Timmermans and Commissioner Jourová 's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems) (Oct. 6, 2015), *available at* http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm (stating that "[t]oday's judgment by the Court is an important step towards upholding Europeans' fundamental rights to data protection").

[34] *See* Article 29 Data Protection Working Party, Statement on the Implementation of the Judgment of the Court of Justice of the European Union in Schrems v. Data Protection Commissioner (Oct. 16, 2015), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (stating that the Working Party "the Working Party is urgently calling on the Member States and the European institutions to open discussions with US authorities in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights").

[35] *See, e.g.*, Letter from Marc Rotenberg to the Editor, N,Y. Times (Oct. 13, 2015), *available at* http://www.nytimes.com/2015/10/13/opinion/digital-privacy-in-the-us-and-europe.html ([I]t is absolutely vital that courts protect fundamental rights. And that is what happened in this case.").

[36] *See* 37th International Privacy Conference, https://www.privacyconference2015.org/ (last visited Oct. 22, 2015).

although I and other close observers of the European privacy scene have been discussing the potential implications of the *Schrems* case for some time, the decision clearly came as a shock to many policy makers and companies in the United States. During a discussion held just last week in the heart of Silicon Valley, a Member of the U.S. House of Representatives who hails from that area of California stated that the *Schrems* decision measured 7.8 on the Richter scale.[37] For those of you not as familiar with earthquakes as they are in California, that is an enormous shock that would seriously test most bridges. It also makes the need for building stronger and more durable bridges that much clearer.

Thus the *Schrems* decision has placed us at a critical juncture where we need to reflect on the deep values that we share, be honest about the nature of our similarities and differences, and assess the steps we need to take in order to develop a truly trusted framework for the transatlantic flow of information.

What Has Been Lost? What Has Been Gained?

Ever since the Snowden revelations made Safe Harbor a target of choice for critics of U.S. surveillance practices, I have had two messages.[38] First, Safe Harbor needed improvements. It needed more transparency, consumers should never have had to pay for dispute resolution, and there were numerous steps that the U.S. side needed to take to make its administration more effective. The U.S Department of Commerce moved quickly to make several of these changes even while the negotiations were still underway. I believe that the even more far reaching improvements that have been under discussion for the past two years will provide a more effective source of privacy protections for consumers in Europe as well as the United States. More on that in a minute.

My other message about Safe Harbor has been that it was the wrong target for arguments that U.S. surveillance practices violate the privacy rights of Europeans. Facebook's membership in the Safe Harbor program was the basic fact that led Max to file his complaint. Yet the ECJ judgment doesn't focus at all on the practices of Facebook. Instead, the judgment recites some of the allegations about U.S. surveillance practices that were made before the Irish High Court,[39] and its holding relies entirely on the absence of findings in the European Commission's adequacy decision concerning surveillance limits under U.S. law,[40] as well as the absence of findings concerning Europeans' redress rights in the United States.[41] Critics of U.S. surveillance

---

[37] *See* Wikipedia, 1906 San Francisco Earthquake (last updated Oct. 21, 2015), *available at* https://en.wikipedia.org/wiki/1906_San_Francisco_earthquake (stating that the 1906 San Francisco earthquake had an estimated magnitude of 7.8 on the Richter scale, caused an estimated 3000 deaths and $10.5 billion in damage (2015 dollars)).

[38] *See* Julie Brill, Commissioner, Keynote Address Before Forum Europe Fourth Annual EU Data Protection and Privacy Conference 6-7 (Sept. 17, 2013), *available at* https://www.ftc.gov/public-statements/2013/09/keynote-address-forum-europe-fourth-annual-eu-data-protection-and-privacy.

[39] *See Schrems v. Data Protection Comm'r*, *supra* note 32, at ¶¶ 26-35.

[40] *See id.* at ¶ 88.

[41] *Id.* at ¶ 95.

practices – and there are many of them – are pleased with the way that the Court took a strong stand regarding the allegations of mass surveillance that were before it.

We should recognize that important protections were lost through the Court's invalidation of the European Commission's decision in 2000 to approve Safe Harbor as a data transfer mechanism. And they will continue to be lost if we do not have a durable and protective mechanism for information flow between the U.S. and Europe. Let me focus on two of these losses. First, the ECJ's decision will make transatlantic data transfers far less transparent. When a company joined Safe Harbor, consumers knew it, advocates knew it, and the entire enforcement community knew it. The United States government publishes a single, authoritative list of every company that filed its Safe Harbor self-certification.[42] Safe Harbor companies also identified themselves as members and publicly committed to follow Safe Harbor's principles. This representation not only added to Safe Harbor's transparency, but also provided the basis for the forty or so companies that the FTC charged with deceiving consumers about their compliance with Safe Harbor.

Some of the alternatives to Safe Harbor do not offer this same level of transparency. For example, model contracts might require companies to file copies of their contracts with a data protection authority, though this is not the case in every Member State.[43] This arrangement simply doesn't compare to the transparency that Safe Harbor provided. And although companies with approved binding corporate rules are listed on the European Commission's website,[44] the details of the rules that each company creates for itself are not public. The relative advantages and drawbacks of these and other means of legally transferring personal data to third countries are part of a longer conversation, and some may not view transparency alone as a sufficient reason to adopt a new mechanism for ensuring safe and protective data flows across the Atlantic. But the loss in transparency is real.

The second loss that stems from the Court's decision is it makes FTC enforcement of companies' transatlantic privacy commitments much more difficult. Simply put, the absence of representations to consumers by companies may limit the FTC's ability to take action against those companies if they misrepresent how they follow European privacy standards – because in the absence of Safe Harbor, there is little reason to make those representations in the first place. The lack of public commitments also makes conduct that harms consumers more difficult to detect. The FTC, with its many years of experience and nearly 100 privacy and data security

---

[42] Dept. of Commerce, U.S.-EU Safe Harbor List, https://safeharbor.export.gov/list.aspx (last visited Oct. 22, 2015).

[43] *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).

[44] *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.

enforcement actions[45] (not counting our 40 actions involving Safe Harbor issues), has been an important and highly expert force. Our law enforcement actions have brought consumer data practices to top executives' attention by developing a body of law that causes companies to think hard about whether their practices respect consumers' expectations.[46] The vast bulk of companies that committed to the Safe Harbor principles have taken their obligations seriously, and developed meaningful internal processes to ensure compliance. The FTC will of course continue with its robust privacy and data security enforcement program, and its past and future actions involving companies that engage in global data flows will still protect EU citizens along with U.S. consumers. But the invalidation of the European Commission's Safe Harbor decision removes the most explicit link between FTC enforcement and our ability to protect European consumers.

The *Schrems* decision also had an important benefit that has not been widely appreciated, at least in the United States. Prior to the decision, in some quarters in the United States, there has been suspicion that discussions about privacy in Europe were veiled attempts at protectionism. I believe the *Schrems* decision should put those suspicions to rest. The decision crystallizes what has been clear – or should have been clear – for a long time about privacy in Europe: it is a fundamental right that Europeans and their Court take very seriously. Where the data practices of *companies* are concerned, this fundamental rights perspective is quite different from the United States. Where the *government's* collection of personal data is concerned, however, 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;[47] 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.[48]

First Steps Forward Post-*Schrems*

So let's turn to the most immediate issue at hand: development of a stronger transatlantic data transfer mechanism. In the two and a half weeks since the ECJ decision was published, I have spoken with many stakeholders on both sides of the Atlantic about these issues, including companies and lawyers in private practice who wonder when the much-discussed negotiations

---

[45] *See* FTC, Privacy and Security Update (2014), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2014 (reporting that the FTC has settled more than 50 data security actions and more than 40 general privacy actions under Section 5).

[46] *See generally* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).

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

[48] *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.

between the European Commission and the United States over a strengthened data transfer framework will conclude. Their eagerness is understandable. Thousands of companies are facing the task of renegotiating contracts, adjusting data flows, or some combination of the two, to ensure that they are transferring personal data legally.

But this is about much more than the immediate issues facing each of the 4,500 companies that must independently determine whether and how they can continue to serve their customers or transfer information about their employees within the confines of the Court's ruling. At a higher level, the stakes also include ensuring the free flow of commerce and information to serve the interests of 800 million consumers across two continents. As the EU Commissioner for Justice, Věra Jourová, aptly said when she spoke about the European Court's decision: "it is important that transatlantic data flows can continue, as they are the backbone of our economy."[49]

I believe we should create a new data transfer mechanism that strengthens the privacy protections that were in the Safe Harbor principles. The seven Safe Harbor principles were already expansive and protective. They provided for notice, choice, access, security, use restrictions, and other protections that one would expect from a baseline privacy regime.[50] Although the text being negotiated by the Commission and the United States has not been made public, I have every reason to believe that both sides understand the need to ensure that these substantive protections are more robust, and that both sides have been working to that end. With strong privacy standards enforceable by the FTC as a foundation, we should create a stronger transatlantic data transfer mechanism that would protect EU citizens' privacy while also providing certainty to business and creating a data transfer mechanism that presents a practical and legal option for companies – particularly small and medium-sized companies – that need to transfer personal data to the U.S. For all of these reasons, I hope that the negotiations come to a speedy and successful conclusion.

Long Term Goals

More long term, 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. From a purely bureaucratic perspective, that separation makes practical sense. It allows different parts of the U.S. government to stay out one another's way. Within this framework, the FTC occupies an important and large – yet well-defined – swathe of the privacy landscape. We carry out much of our privacy enforcement program under the banner of our general consumer protection authority, and we are a purely civil law enforcement agency. As a result, the interests

[49] European Commission Statement, *supra* note 34.

[50] *See* Dept. of Commerce, Safe Harbor Privacy Principles (July 21, 2000), *available at* http://export.gov/safeharbor/eu/eg_main_018475.asp.

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 an ongoing, robust 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.[51] Many security experts and privacy advocates argued, however, that any other plausible arrangement would introduce vulnerabilities into devices and networks that would put consumers' data and devices at an unacceptable risk.[52] I came down on the side 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.[53] Fortunately, the White House recently stated that it would not seek legislation to require companies to install technologies to provide access to unencrypted communications.[54] Still, the debate over whether to enact such legislation is likely to continue in other venues. My hope and expectation is that this debate in the U.S. over law enforcement's encryption challenges 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.[55] Some reform proposals to modernize this law and restrict law enforcement access have broad support in Congress.[56] These proposals would essentially prohibit civil law enforcement agencies like the FTC from

---

[51] *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.

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

[53] *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").

[54] *See* Nicole Perlroth and David E. Sanger, *Obama Won't Seek Access to Encrypted User Data*, N.Y. TIMES (Oct. 10, 2015), *available at* http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html.

[55] *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.

[56] *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).

going to service providers to obtain communications content during their investigations[57] – something that they can do now but only in limited circumstances. I took the view that the FTC has not in fact used this authority, we don't not need this authority, and that allowing civil law enforcement agencies to use such authority raises significant consumer privacy and constitutional concerns.[58]

As these examples illustrate, in the United States, we are engaged in a robust conversation about these issues. I believe Europeans 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. The ECJ's decision suggests that the United States and Europe should have an honest dialogue about the "essential equivalence" of all of these data practices within companies, as well as within our law enforcement and national security agencies.

* * * * *

But let me return to Nico's original question, regarding the Internet of Things and big data analytics. 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 focus on the right questions and understand both the technical details and policy implications of analytics,[59] algorithms,[60] and connected devices.[61] We have incorporated the position of a chief technologist into our agency, and have brought in academics of global renown in the fields of computer science and cybersecurity to serve in that capacity and help us address these critical issues. 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 what data the

[57] *See* H.R. 699, *supra* note 56; 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).

[58] *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.

[59] *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.

[60] *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.

[61] 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.

systems collect and how they use it. And while we have developed best practices for businesses that are creating connected devices and other new technologies,[62] we have also brought enforcement actions against companies that fail to take reasonable steps to protect sensitive data that flows from these devices,[63] or collect or use the data in ways that defy consumers' expectations or harm them. As part of a 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 we are adequately protecting consumers with respect to these new technologies. Let me also be absolutely clear about another point: 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. Indeed, the call for additional legislative protections for consumer privacy in the United States is similar to the call here in Europe to update and refurbish the 1995 Directive through adoption and implementation of the General Data Protection Regulation.

For several years, I and my fellow 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.[64] 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.[65] 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.[66] And the FTC has pressed Congress to enact federal data security legislation.[67] The case for enacting these laws was compelling before the *Schrems*

---

[62] *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).

[63] *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.

[64] *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.

[65] *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.

[66] *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.

[67] *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).

ruling. 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.

Building more trust in transatlantic data flows and ensuring privacy and security protections for our highly connected, data-intensive world are very big tasks. The FTC cannot and should not do this work alone. Nor can or should the European DPAs. Next week the global privacy community will discuss proposals from the EU-U.S. Privacy Bridges Project[68] concerning a series of concrete steps that EU and U.S. regulators and stakeholders can take together to meet high standards of privacy protection.

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 have 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 in this same honest discussion. All of us – companies, policy makers, advocates, academics and researchers, in Europe and America – need to get involved in this conversation. If we start engaging in an honest dialogue, I believe we can, over the long term, forge a path towards building truly robust and durable bridges that will allow us to face our common challenges together, so we can more effectively protect the data and privacy of our citizens.

Thank you.

[68] *See* EU-U.S. Privacy Bridges, http://privacybridges.mit.edu/ (last visited Jaun. 2009).