Privacy Shield and the Future of Europe

By Julie Brill, Hogan Lovells Partner and Co-Lead Global Privacy and Cybersecurity Practice

Delivered to the Institute of International and European Affairs

Dublin, Ireland

July 12, 2016

I. Introduction

Thank you for that extremely kind introduction. And I'd like to thank the Institute of International and European Affairs for inviting me to speak today on a set of issues that are near to my heart. Our timing could not be more appropriate.

For the second time in less than a month, Europe stands on the threshold of history. As many Europeans are still trying to wrap their heads around the idea of a union without Britain, the European Commission has been moving toward ratification of a landmark data-protection agreement with the United States.

The agreement, known as Privacy Shield, will provide European citizens with unprecedented protections for their personal and commercial data. It will also make Europe a vital hub in the global flow of digital information.

Earlier today, European Commissioner for Justice Věra Jourová and U.S. Secretary of Commerce Penny Pritzker signed the Privacy Shield agreement, marking its final approval and opening the door on a new era of safe, secure digital commerce for European citizens and businesses.

But immediately following this historic step, Privacy Shield is certain to face legal challenges, leaving the courts to decide its fate. These decisions will have a monumental impact on the future of Europe, and on the EU's place in the global economic hierarchy.

Before I get into the weeds — and, as a former United States Federal Trade Commissioner, I assure you, I can get into the weeds — I want to take a moment to give you a preview of what we'll be discussing today.

First, I'll briefly describe how Privacy Shield came about, how it differs from its forebearer, the Safe Harbor, and how it provides essentially equivalent protections to those enjoyed by Europeans in their own countries. Second, I'll discuss the ways that Europe's attitude toward Privacy Shield strikes at the future it sees for itself in the global economy and community. Third, I'll argue that the ratification of Privacy Shield is essential precisely because it's not a panacea, but one step in the continuing evolution of the law – which must evolve to keep pace with a digital ecosystem that increases in complexity by the day.

II. Background

There's never been a more important moment for privacy protection than the one we face today, both with regard to data sharing, and to our broader economies. The European Union

and the United States have an opportunity to embrace our shared belief in free market economic principles and, more essentially, the democratic process. To quote my former boss, President Obama, "What binds us together is greater than what drives us apart."[1] I believe that the Privacy Shield agreement captures these common values, and that's why I support its ratification and implementation.

I do not take lightly notions of privacy. In the sometimes-pitched battle between the machinery of the free market and consumers' rights, I have staked my career on defending the latter. Before serving as a Commissioner of the U.S. Federal Trade Commission, I spent 20 years enforcing privacy laws at the state level, first as Assistant Attorney General for Consumer Protection and Antitrust in Vermont, and then as Chief of Consumer Protection and Antitrust in North Carolina.

In my six years as a Commissioner at the FTC, the agency brought hundreds of enforcement actions against companies, including many tech giants,[2] that we believed had failed to keep consumers' data reasonably secure, misrepresented their data collection and use practices, treated consumers and their data unfairly, and/or violated one of the many specific laws designed to protect sensitive data. We obtained millions of dollars in penalties and restitution in these privacy and data security actions, and we placed numerous companies under 20-year orders with robust injunctive provisions relating to their privacy and data security practices.[3]

Throughout my tenure, I championed the consumer's right to transparency, notification, and privacy — efforts that were recognized when I was named the 2014 Privacy Leader of the Year by the International Association of Privacy Professionals.[4] Since leaving the Federal Trade Commission in March, I have continued my advocacy work, including appealing for more

---

[1] BARACK OBAMA, THE AUDACITY OF HOPE: THOUGHTS ON RECLAIMING THE AMERICAN DREAM 2 (2006).

[2] See, e.g., Twitter, Inc., No. C-4316 (F.T.C. Mar. 2, 2011) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf (last visited July 6, 2016); Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012) (decision and order), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (last visited July 6, 2016); Google, Inc., No. C-4336 (F.T.C. Oct. 13, 2011) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf (last visited July 6, 2016); MySpace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacedo.pdf (last visited July 6, 2016).

[3] See, e.g., Press Release, F.T.C, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (August 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (last visited July 6, 2016); Press Release, F.T.C, LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False (March 9, 2010), https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states (last visited July 6, 2016).

[4] Press Release, Int'l Ass'n Privacy Profs., FTC Commissioner Julie Brill Honored with International Association of Privacy Professionals 2014 Privacy Leadership Award (March 7, 2014), https://iapp.org/about/ftc_commissioner_julie_brill_honored_with_international_association_of_priv/ (last visited July 6, 2016).

stringent regulations governing the U.S. government's ability to access electronic data about its citizens.[5]

I recognize that, in detailing my work history, I may sound like I'm here looking for a new job, but that is far from the case — I love my work and I'm very happy at Hogan Lovells. Instead, I provide this career summary to demonstrate that when I say that I believe Privacy Shield is an effective and essential framework for the protection of European consumer data, I say it with the street cred of a proven and tireless consumer advocate.

III. So what is Privacy Shield?

So what is Privacy Shield? What protections does it offer, and why do they matter? And how did we arrive at a point where we have been operating, up until today, without a seamless legal framework for our transatlantic data flows? To answer these questions, I'll need to provide a brief history.

Back in 2000, the United States Department of Commerce and the European Commission finalized a privacy framework called Safe Harbor.[6] It was designed to protect the rights of European citizens as their data traveled across the Atlantic. American companies that adhered to Safe Harbor were allowed to collect and use data about European consumers and employees, and store the data on U.S. servers.[7] By October of last year, some 4,500 U.S. companies, large and small, were relying on Safe Harbor to handle the data of tens of thousands of European and American employees and to do business with millions of European citizens.[8]

Then, in October, the Court of Justice of the European Union invalidated Safe Harbor, holding that it didn't provide Europeans with the levels of protection to which they were entitled as EU citizens.[9]

But while the Court of Justice's decision in *Schrems v. Data Protection Commissioner* sounded the death knell for Safe Harbor, negotiations on an updated data security framework between the U.S. and the EU had already begun,[10] two years before *Schrems*, after Edward Snowden revealed that U.S. intelligence agencies had been collecting personal consumer data

---

[5] Julie Brill, *It's time to update the Electronic Communication Privacy Act (ECPA)*, The Hill: Congress Blog (May 25, 2016, 11:00 AM), http://thehill.com/blogs/congress-blog/technology/281106-its-time-to-update-the-electronic-communications-privacy-act.

[6] Letter from John F. Mogg, Dir. DG Internal Mkt., European Comm'n, to Robert LaRussa, Acting Under Sec'y for Int'l Trade, U.S. Dept. of Com. (DG Markt/E-1 D(2000)168).

[7] Welcome to The U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, Export.gov, http://www.export.gov/safeharbor/ (last visited July 7, 2016).

[8] Martin A. Weiss & Kristin Archick, CRS, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, 6 (February 12, 2016), https://www.fas.org/sgp/crs/misc/R44257.pdf (last visited July 6, 2016).

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

[10] Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision (October 6, 2015), https://www.commerce.gov/news/press-releases/2015/10/statement-us-secretary-commerce-penny-pritzker-european-court-justice (last visited July 6, 2016).

held by American companies. The *Schrems* decision certainly added urgency to these negotiations, but the writing had been on the wall since Snowden: European policy makers and privacy advocates believed that Safe Harbor's protections were no longer adequate.[11]

Privacy Shield is the result of the negotiations that began in 2014, a new framework designed to replace and improve upon Safe Harbor.[12] I believe it is the framework that Europeans deserve today. Privacy Shield strengthens consumer protections with regard to both government and commercial access to data. In doing so, it addressees the European Court of Justice's two major concerns about Safe Harbor: first, it outlines the fortifications to existing safeguards against government access to personal data for the purposes of national security surveillance; second, it provides clear, inexpensive avenues of redress for individuals concerned that their data is being used improperly. These provisions are designed to meet the Court's demands that the protections governing any transfer of Europeans' data out of the EU be "essentially equivalent" to those found in European law.[13]

To understand Privacy Shield, and why its protections are adequate, it is first important to understand the requirements that businesses and government agencies face under the current regime of American privacy law. It's true that the U.S. has no single law like the baseline data protections found in most EU member states. But taken as a whole, U.S. laws and regulations do provide a layered assemblage of strong consumer safeguards. Indeed, U.S. law was clearly the inspiration for many of the guiding principles that informed the drafting of the European General Data Protection Regulation, including an emphasis on data security and breach notifications, a focus on heightened protections for children's data, and a prioritization of deidentification of sensitive data.

Where government collection of personal data is concerned, the idea of a fundamental, constitutional right to privacy is a cornerstone of American law, deeply woven into our social and legal fabrics. Recently the right to privacy has been extended through the courts to include new technologies and new forms of communication.[14] The Judicial Redress Act,[15] the USA

---

[11] *See,* Memo, Eur. Com., Informal Justice Council in Vilnius (July 19, 2013), http://europa.eu/rapid/press-release_MEMO-13-710_en.htm (Last visited July 11, 2016); European Parliament resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, P7_TA(2014)0230 at 38.

[12] U.S. Dep't of Commerce, EU-U.S. Privacy Shield, https://www.commerce.gov/privacyshield (last visited July 7, 2016). Press Release, U.S. Dept. Com., Statement from U.S. Secretary of Commerce Penny Pritzker on Release of EU-U.S. Privacy Shield Text, https://www.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-release-eu-us-privacy (last visited July 7, 2016).

[13] *Shrems* at para. 73.

[14] *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, https://www.congress.gov/bill/114th-congress/housebill/2048/text?q=%7B%22search%22%3A%5B%22%5C%22hr2048%5C%22%22%5D%7D&resultIndex=1&over view=closed; Presidential Policy Directive – Signals Intelligence Activities (PPD-28) (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Freedom Act[16] and President Obama's Policy Directive 28,[17] all adopted in the wake of the Snowden revelations, honor and strengthen this tradition by providing new limitations on the way data is collected and used by U.S. intelligence services. The Judicial Redress Act, which explicitly extends the protections of the Privacy Act to foreign citizens, is particularly noteworthy in this discussion.

Other individual statutes protect information about children,[18] finances,[19] medical data,[20] and student data,[21] as well as information used to make decisions about consumers' credit, insurance, employment and housing.[22] At the state level, approximately 60 privacy laws were passed last year alone.[23] The Attorneys General of each of the 50 states, as well as a legion of federal agencies – led by the FTC – each have broad imperatives to enforce these laws and bring to account those whose actions do harm to consumers.

Privacy Shield clarifies this amalgam of restrictions already governing data flows in the United States. With respect to government surveillance, the Office of the Director of National Intelligence and the Department of Justice have provided letters describing the limitations on government access to data for intelligence and law enforcement purposes.[24] These letters are significant on two levels. First, they lay out the U.S. Government's binding commitments to apply the same protections to European citizen data that it applies to its own citizens' data. These commitments include the government's fortification of citizens' protections in the USA Freedom Act and the U.S. Foreign Intelligence Surveillance Act, and the improvements in the operation of the U.S. Foreign Intelligence Surveillance Court. Second, these letters demonstrate that the United States, and in particular the intelligence and law enforcement communities, take the European Court of Justice's concerns seriously.

---

[15] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282.

[16] Uniting and Strengthening America By Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

[17] Press Release, the White House, Presidential Policy Directive/PPD-28 — Signals Intelligence Activities (January 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (last visited July 7, 2016).

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

[19] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-09.

[20] 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.).

[21] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

[22] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*

[23] State Laws Related to Internet Privacy, Nat'l Conf. State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (last visited July 7, 2016).

[24] Letter from Robert S. Litt, General Counsel, Office of the Dir. Nat. Intelligence, to Justin S. Antonipillai, Counselor, U.S. Dept. Com., and Ted Dean, Dept'y Assist. Sec'y, Int'l Trade Admin. (Feb. 22, 2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf (last visited July 7, 2016); Letter from Bruce C. Swartz, Deputy Assistant Att'y Gen. and Counselor for Int'l. Aff., U.S. Dept. Just., to Justin S. Antonipillai, Counselor, U.S. Dept. Com., and Ted Dean, Dept'y Assist. Sec'y, Int'l Trade Admin. (Feb. 19, 2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-7_en.pdf (last visited July 7, 2016).

Of course, such assurances are only as good as one's capacity to enforce them. To that end, Privacy Shield mandates the creation and appointment of an Ombudsperson, within the State Department, who will operate independently of the national security agencies and be available exclusively to Europeans.[25] Any European citizen with concerns about U.S. surveillance of his or her data may file a complaint to the Ombudsperson, who will in turn verify that any surveillance measure has been implemented in accordance with law, and correct any anomalies or violations of the citizen's rights. It is worth noting that the ombudsperson bears a striking resemblance to the National Oversight Commission — France's own solution to the balancing of individual rights and national security.[26]

On the commercial side, Privacy Shield significantly enhances protections that had been built into Safe Harbor. For instance, Privacy Shield requires data controllers to obtain consent from Europeans before they share data with third parties, including affirmative, express consent to share sensitive data such as health information. Privacy Shield also compels data controllers to allow Europeans to access, correct, or delete their transferred data. Crucially, data controllers will have to require their business partners who receive information about Europeans to live up to these principles, as well.

Finally, a raft of new procedural safeguards will make it easier – and a lot less expensive – for European consumers to pursue justice when they have been wronged by a participating company. For instance, U.S. companies that sign onto Privacy Shield must agree to provide independent recourse mechanisms at no cost to the complainant. Should this measure fail, individuals can then take the company to binding arbitration — once again at no cost to the individual – or to court.

Since Privacy Shield's debut, in draft form, three months ago, a number of stakeholders in Europe have analyzed and critiqued it. Most significantly, Europe's data protection watchdogs, collectively known as the Article 29 Working Party, welcomed Privacy Shield's "significant improvements," while suggesting some clarifications and expressing other continuing concerns.[27] The negotiating parties have spent the past three months enhancing Privacy Shield to address the Article 29 Working Party's concerns. The resulting improvements include added restrictions on the ability of Privacy Shield companies to retain data about EU citizens, and a clearer articulation of the extent of the Ombudsperson's independence from the Administration.[28]

---

[25] *See* EU-U.S. Privacy Shield Ombudsperson Mechanism Annex A, at 2-3.

[26] Julie Brill et Winston Maxwell, *Les « Cnil » européennes tirent exagérément sur le nouveau bouclier « Privacy Shield »,* Edition Multimédi@ 145 (May 16, 2016); Julie Brill and Winston Maxwell, *Criticisms of Privacy Shield Fail to Recognize Shortcoming of Europe's Own Intelligence Laws,* Bloomberg Law: Privacy and Data Security (June 14, 2016).

[27] Art. 29 Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 16/EN WP 238 at 2 (April 13, 2016).

[28] Eur. Com. Decision No. XXX, (on the adequacy of the protection provided by the EU-U.S. Privacy Shield), http://cdn.arstechnica.net/wp-content/uploads/sites/3/2016/06/2016-06-28-COM-AC_DR2016D045249-08_EN-text-for-opinion-1.pdf (last visited July 11, 2016) (unofficial version).

As I have traveled across Europe over the past months, I have heard various stakeholders voice an additional concern. They point out that, because Privacy Shield does not have the status of a treaty, a new U.S. Administration could water down Privacy Shield's protections. They are correct that Privacy Shield is not a treaty. The commitments of its signatories, however, *are* binding – on the part of both the U.S. government and companies that voluntarily sign up. It is hard to conceive of a U.S. Administration that would *not* eagerly embrace Privacy Shield and work hard to implement its highest levels of protection. But if such an anomaly occurs, there is a failsafe. The new framework requires Europeans and Americans to consult at least annually on the framework's operation. And if the European Commission believes that the U.S. is violating its commitments, the Commission is empowered to suspend Privacy Shield.[29]

IV. Europe's charge

I'd like to take a moment here to answer a question that may be nagging at some of you. Post-*Schrems*, Europeans have still been able to log onto Facebook, and send out tweets, to their heart's content. The data has continued to flow, even without Safe Harbor in place. So, with Safe Harbor invalidated, what set of rules protects that data?

For the past eight months, businesses that previously relied on Safe Harbor have been permitted to employ standard contractual clauses, binding corporate rules or some other pre-approved mechanisms to ensure that their data transfer practices meet the requirements set out by the EU. Yet these data transfer mechanisms – unlike Privacy Shield – are opaque. For example, companies with approved binding corporate rules are listed on the European Commission's website, but the details of the rules that each company has created are not publicly available.[30] And it can be similarly difficult to know which companies use standard contractual clauses. In addition, these mechanisms can be expensive to implement, which makes them harder for small- and medium-sized enterprises to use. This is especially harmful because many SMEs on both sides of the Atlantic depend on the free flow of information to sell goods and services around the world, build global workforces, and take advantage of low-cost cloud computing resources.

Casting further uncertainty, Irish Data Protection Commissioner Helen Dixon has just referred to the courts the question of whether Standard Contractual Clauses are adequate under the European law.[31] Businesses, which rely on a stable landscape to deploy resources and

[29] Privacy Shield, EU-U.S., Feb. 23, 2016, available at https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf (last visited July 11, 2016).

[30] List of Companies for which the EU BCR cooperation procedure is closed, ec.europa.eu, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last visited July 6, 2016).

[31] Press Release, Statement by the Office of the Data Protection Commissioner in respect of application for Declaratory Relief in the Irish High Court and Referral to the CJEU (May 25, 2016), https://www.dataprotection.ie/docs/25-05-2016-Statement-by-this-Office-in-respect-of-application-for-Declaratory-Relief-in-the-Irish-High-Court-and-Referral-to-the-CJEU/1570.htm (last visited July 6, 2016).

make investments, are nervously watching this development and hoping the ground does not shift beneath them again.

We can already see the havoc wrought by this state of legal limbo. Adobe, Pepsi, and Unilever — not exactly unsophisticated players — were all fined by German regulators in June for continuing to rely on Safe Harbor rather than setting up alternative legal channels.[32] And in April, cloud storage company Box teamed[33] with IBM to allow companies to store data in regional data storage facilities on European soil, following a similar arrangement between Microsoft and Deutsche Telekom.[34] While not in themselves bad news, these developments may speak to the degree of uncertainty businesses feel in the current climate, and the seriousness with which they are responding to a perception of increasing European insularity. Forcing businesses to localize their data warehousing and split their storage capabilities will not foster robust competition or be an economically viable long-term solution. But more importantly, if Europe were to turn further toward insularity, it would create a dangerous international precedent. Regimes around the world could point to the continent to justify their own data localization laws and their ensuing efforts to increase government access to citizens' data – often without the safeguards that exist in democracies like the U.S. and EU member states.

When speaking about the impact of *Schrems* last October*,* Věra Jourová, the EU Commissioner for Justice who signed Privacy Shield earlier today, said, "It is important that transatlantic data flows can continue, as they are the backbone of our economy."[35] She recognized that the free flow of data underpins how we learn, how we communicate, how we do business.

Recognizing these fundamental truths, just last week, the member states of the European Union voted to approve Privacy Shield.[36] And today, as the European Commission and the U.S. Department of Commerce announced final approval of the new framework, governments on both sides of the Atlantic have affirmed that because data is the lifeblood of the new economy, its transfer requires a clear set of guidelines. We need rules that allow consumers to consent to or reject overtures to collect or use their data, and a transparent set of mechanisms for

---

[32] Press Release, The Hamburg Comm'r for Data Protection and Freedom of Info., Inadmissible data transfer to the USA: First fines are final, other cases still pending (June 6, 2016), https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-06-06_Data-Transfer_to_the_USA.pdf (last visited July 6, 2016).

[33] Press Release, IBM and Box to Enable Local Data Storage in Europe and Asia with Box Zones and IBM Cloud (Apr. 12, 2016), http://www-03.ibm.com/press/us/en/pressrelease/49513.wss (last visited July 6, 2016).

[34] Press Release, Microsoft Announces Plans to Offer Cloud Services from German Datacenters (Nov. 11, 2015), https://news.microsoft.com/europe/2015/11/11/45283/#sm.0001uecob412szfsew7dnfmfl4jma (last visited July 6, 2016).

[35] 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), http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm (last visited July 6, 2016).

[36] Press Release, Eur. Com., Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield (July 8, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm (last visited July 11, 2016).

consumers to seek recourse when they feel that their fundamental rights to privacy have been abridged.

Privacy Shield is not perfect — no large-scale regulatory framework is, especially not on the first pass. But perfection is not what the moment calls for. Instead, we should view Privacy Shield as a living framework. As I noted, the U.S. Department of Commerce and EU Commission will engage in ongoing consultations about its effectiveness, and about whether the parties are living up to their commitments. The European Data Protection Authorities and the U.S. Federal Trade Commission will also hold continual discussions about enforcement issues under the framework. The ultimate test of Privacy Shield's effectiveness will be how well it works in practice in the months and years to come.

As for today, I am confident in saying that the protections provided to European citizens under Privacy Shield are "essentially equivalent" to those they enjoy on their own soil. The final decision about Privacy Shield's adequacy will be made by the European Court of Justice. I am hopeful that the Court will provide itself with the means to appreciate the full spectrum of protections built into Privacy Shield as they adjudicate the near-certain lawsuit that will be brought by well-intentioned privacy activists, likely beginning tomorrow.

V. Next steps

As the merits of Privacy Shield are debated and determined, both at the court in Luxembourg and in the court of public opinion, it's just as important to keep our eye on the ultimate prize — continually guaranteeing consumers the right to privacy, even as the ground beneath us relentlessly shifts. This requires more than statutes and agreements that govern oversight and data stewardship. It requires intelligence and vigilance, innovation and collaboration. How we foster a safe, fertile environment for the flow of data depends on our willingness to work together to adapt to the changes brought by ever-evolving technologies.

For an example I point you to the Internet of Things. We are connecting nearly everything to the Internet these days – from cars and buildings to clothing and light bulbs. The pace and scale of these changes are breathtaking. Cisco reports that there are 25 billion networked devices in the world today and predicts that there will be 50 billion by 2020.[37] Sensors in these devices, along with our smartphones, tablets, and computers, generate twice as much data today as they did just two years ago, and this trend shows no evidence of slowing down. To my eye, this can all be to the good. From enabling cities to better maintain their infrastructures to developing effective treatments for some of the most intractable diseases, we stand at the brink of possibility.

But as we add networked devices to our homes, classrooms, and clothes, much more sensitive data will also be collected. User interfaces on devices will shrink or disappear, making it more difficult for consumers to know and keep track when data is being collected, or to

[37] DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING (April 2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (last visited July 7, 2016).

exercise control over its movement. These developments will pose difficult challenges for privacy, security, and fairness in our societies.[38]

Without data security, there is no such thing as privacy. My former agency, the U.S. Federal Trade Commission, noted that the Internet of Things' network of connected devices is only as secure as its weakest link, and the expansion in threat vectors creates a risk not only to data, but also to the devices themselves.[39] If we are serious about protecting the privacy of consumers, we must focus on the damage done by an attack that threatens data and device as much as the damage done by unauthorized transfers to a third-party vendor. The geometric rate of increase in devices used and data collected makes it all the more essential to reach outward to our allies, rather than shrink inward and batten down the hatches.

The opportunity we have now is to balance the competing interests that complicate decisions in any free society. I believe that within these larger issues presented by newer data-intensive technologies, and the highly connected world they create, the United States and Europe may be able to forge a constructive dialogue. Here we may find common approaches to simultaneously foster innovation and address the challenges these technologies pose to fundamental principles of privacy, security, and fairness in our societies.

Once we have a new data transfer mechanism in place, and once we begin an honest conversation about the ways in which our law enforcement and intelligence data collection practices are essentially equivalent, the United States and Europe will be primed to face the challenges that these brave new developments present. Then, we will position ourselves to protect our citizens' data, and their privacy, for the future.

[38] Julie Brill, *Regulators Must Guide the Internet of Things*, NY Times: Room for Debate (Sept. 8, 2013), http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things (last visited July 11, 2016).

[39] F.T.C STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (last visited July 11, 2016).