The Federal Trade Commission and the Future of Privacy and Data Security
University of California, Berkeley School of Law
Berkeley Center for Law & Technology
September 15, 2015

Thank you, Dean Choudhry, for your kind introduction. And thank you to Jim Dempsey and the Berkeley Center for Law & Technology (BCLT) for hosting me this afternoon. Although the pathbreaking work by scholars like Deirdre Mulligan, Paul Schwartz, Ken Bamberger, Chris Hoofnagle and others is the real draw for me, the hills, the views of the Bay, and the food don't hurt, either. And I'm glad to speak with so many students while I'm here. If memory serves, around this time of year, many of you are suffering through on-campus interviews, callbacks, clerkship applications, and the like. At least exams are a long way off.

I promised Jim that I would speak about the *future* of privacy and data security. But, since some of you might not be familiar with the Federal Trade Commission (FTC) and how we have become involved in privacy and data security, I would like to begin with a brief look at the FTC's past.

The FTC is an independent, bipartisan commission. For administrative law buffs, the Supreme Court affirmed our independent status back in 1935 through its decision in *Humphrey's Executor*.[1] The FTC is first and foremost a civil law enforcement agency. We are the nation's leading consumer protection agency, and we share competition enforcement with the Department of Justice. Under authority given to us in 1938, the FTC is responsible for protecting consumers from a broad range of "unfair or deceptive acts or practices."[2] Under this authority in Section 5 of the FTC Act, we have brought hundreds of cases against companies for making deceptive claims in advertising. We have shut down scams that falsely promise to deliver credit repair, mortgage relief, business opportunities, and other services that predominantly target vulnerable consumers. We even run the Do Not Call list, which Dave Barry has called the most popular government program since the Elvis stamp.[3] Indeed, Congress has passed laws that ban specific kinds of harmful practices, as is the case with robocalling and abusive telemarketing practices.[4] But Section 5 itself is broad and flexible and applies even when more specific statutes are on the books.

Section 5 is also the FTC's main workhorse when it comes to privacy and data security. In the late 1990s, as the commercial Internet was taking off (and many of you were still in grammar school), the FTC recognized that the personal information that was flowing online as part of commercial transactions could cause real harm to consumers when companies fail to protect it appropriately or use it in ways that are contrary to what companies tell consumers.

---

[1] Humphrey's Executor v. United States, 295 U.S. 602 (1935).

[2] 15 U.S.C. § 45(a).

[3] *See* Dave Barry, *Idea for Telemarketers: Hang Up and Go Away*, DESERET NEWS (Aug. 31, 2003 12:00 a.m. MDT), *available at* http://www.deseretnews.com/article/1006979/Idea-for-telemarketers-Hang-up-and-go-away.html?pg=all.

[4] *See* Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. 6101-6108 and Telemarketing Sales Rule, 16 C.F.R. Part 310.

Over the past 15 years or so, the FTC has brought nearly 100 actions under Section 5 protecting millions of consumers – in the United States, Europe, and elsewhere – from deceptive and unfair data practices. We have used this authority to bring enforcement actions against well-known companies like Google, Facebook, Twitter and Snapchat.[5] We have also brought cases against companies that are not household names, but violated the law by spamming consumers,[6] installing spyware on their computers,[7] failing to secure consumers' personal information,[8] deceptively tracking consumers online,[9] violating children's privacy,[10] and inappropriately collecting information on consumers' mobile devices.[11] Most importantly, the broad reach and remedial focus of Section 5 allows the FTC to protect consumers from harm as new technologies and business practices emerge.

The FTC is also deeply engaged in policy development. Congress gave us the authority to order companies to submit "special reports" to us, often including proprietary and confidential information, so we can examine important trends affecting consumer protection and competition in the economy.[12] The FTC recently used this authority in the privacy arena to order nine data brokers to provide information about their data collection use practices. The information that we obtained formed the basis for one of the first in-depth studies of an industry that plays a vital role in the digital economy but is all but invisible to consumers.[13]

---

[5] *See, e.g.*, Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf; Facebook, Inc., C-4365 (F.T.C. July 27, 2012) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; 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; Twitter, Inc. C-4316 (F.T.C. Mar. 2, 2011) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf.

[6] *See, e.g.*, FTC v. Flora, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011) (permanent injunction), *available at* https://www.ftc.gov/system/files/documents/cases/140529floraorder.pdf.

[7] *See, e.g.*, FTC v. CyberSpy Software, LLC, et al., No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), (stipulated final order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100602cyberspystip.pdf.

[8] *See* FTC v. Bayview Solutions, LLC, Case 1:14-cv-01830-RC (D.D.C. Aug. 27, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/111014bayvieworder.pdf *and* FTC v. Cornerstone and Co., LLC, Case 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/150413cornerstoneorder.pdf.

[9] *See, e.g.*, Epic Marketplace, Docket No. C-4389 (F.T.C. Mar. 19, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacedo.pdf.

[10] *See, e.g.*, United States v. Artist Arena, LLC, No. 12-CV-7386 (S.D.N.Y. Oct. 3, 2012) (stipulated final order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121003artistarenadecree.pdf.

[11] *See* United States v. Path, Inc., No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (consent decree and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf; HTC America, Inc., C-4406 (F.T.C. June 25, 2013) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf.

[12] *See* 15 U.S.C. § 46(b).

[13] *See generally* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [DATA BROKER REPORT]

We issue reports and policy recommendations on key issues, informed by public workshops that engage industry stakeholders, academics, advocates, and all levels of government. Among the many significant privacy reports and policy recommendations we've issued in the past few years is our framework for rethinking consumer privacy in a rapidly changing digital society,[14] and our report earlier this year about our initial examination of the potential benefits and privacy and security risks presented by the Internet of Things.[15]

The privacy and data security protections that the FTC has been enforcing under Section 5 for nearly two decades are becoming more important to consumers and companies. The challenges presented in this critical area are also evolving. They are becoming more subtle, more global, and more intertwined with other areas of law. At the same time, many of the basic principles that the FTC has developed over the years apply to new technologies and business models, and Section 5 will remain a vital source of consumer protections in the years ahead.

I'd like to discuss three of the most important privacy and data challenges that are on the FTC's agenda now, and likely will be for several years to come.

Internet of Things

Let's start with the Internet of Things. The Internet of Things is the next large evolutionary step beyond the Internet of PCs, laptops, and smartphones. Cars, appliances, pieces of clothing, and many other everyday "things" are being connected to networks. This has brought about very rapid growth in the number of networked devices. Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people connect to the Internet.[16] Experts estimate that by the end of this year there will be 25 billion connected devices, 50 billion by 2020, and eventually 200 billion.[17]

All of this connectivity brings the possibility of tremendous convenience. Already, a consumer sitting in her office can turn down the heat in her home or turn on the air conditioning

---

[14] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (preliminary staff report) (2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers.

[15] FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 29-46 (staff report) (2015), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [IOT REPORT].

[16] 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. These estimates include all types of connected devices, not just those aimed at the consumer market.

[17] *Id.*; Quentin Hardy, *Intel, Qualcomm and Others Compete for "Internet of Things" Standard*, N.Y. TIMES BITS BLOG (July 8, 2014 12:01 a.m.), *available at* http://bits.blogs.nytimes.com/2014/07/08/standard-behavior-in-an-internet-goldrush/.

in her car while she is still in a meeting, or peer into her basement from across the globe to see whether a recent storm caused flooding.

But the IoT is about much more than convenience. It is also about the data that will be generated by tens of billions of sensors. The data that we collect from the Internet of Things, and the insights we draw from this data, could help solve some of the biggest challenges that we face as a society. In the hands of scientists and analysts, IoT data could help us find ways to use energy more efficiently, avoid traffic jams, stay healthier longer and with less expense, and better predict and manage public health emergencies.[18]

The catch is that much of this data will be deeply personal, and say a great deal about us as individuals. Soon, streams of IoT data will reveal whether we're at home and what we're doing there. They will record how much we've exercised, when we've gained a few pounds, and how well we sleep. They'll log our vital signs, and help us manage our diabetes, heart and other health conditions.

At the same time, as Google's Chairman, Eric Schmidt reportedly said earlier this year, "the Internet will disappear."[19] That is, we'll all carry, wear, walk by, and use so many devices that are connected all the time that the idea of a "network connection" will become an anachronism. Just as we forget about shifting gears in our car once we have an automatic transmission, we'll forget about devices being in a connected state. Connectivity will just be part of how things work.

The development of the Internet of Things – and all the data that will flow from it – also creates some formidable privacy and security challenges. Let me focus on data and device security. The need to secure IoT devices, and the data that they collect and transmit, is pretty clear. Cars, medical devices, appliances, and other IoT gadgets will be conjoined with our physical safety. If attackers take control of these devices, they can cause immediate physical harm.[20] And, of course, privacy is mostly hopeless if IoT devices and services don't keep data secure.

I am deeply concerned about IoT security. Many of the companies entering this marketplace do not have track records of producing secure software and devices. Here's a statistic that should raise alarm about privacy and security risks in the Internet of Things: 90 percent of connected devices are collecting personal information, and 70 percent of them are

---

[18] Public Health Watch, *How A Computer Algorithm Predicted West Africa's Ebola Outbreak Before It Was Announced*, PUBLIC HEALTH WATCH (Aug. 10, 2014), http://publichealthwatch.wordpress.com/2014/08/10/how-a-computer-algorithm-predicted-west-africas-ebola-outbreak-before-it-was-announced/.

[19] 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/.

[20] *See, e.g.*, Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015 6:00 a.m.), *available at* http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Nathanael Paul & Tadayoshi Kohno, *Security Risks, Low-Tech User Interfaces, and Implantable Medical Devices: A Case Study with Insulin Pump Infusion Systems*, *in* PROCEEDINGS OF THE THIRD USENIX WORKSHOP ON HEALTH SECURITY AND PRIVACY (2012), *available at* http://homes.cs.washington.edu/~yoshi/papers/user-interface-security.pdf.

transmitting this data without encryption, according to a recent study by Hewlett-Packard.[21] The FTC is reaching out to companies to offer concrete guidance about security, but there will inevitably be cases in which the FTC needs to take action. And, let's face it: you're law students, I'm an enforcement official, and you probably want to hear about what happens when things go wrong. So here are a couple of examples.

In one case, we believed that the defendant company's Internet-connected cameras were vulnerable to having their feeds hijacked.[22] And, indeed, around 700 private video feeds, some of which included images of children and families going about their daily activities in their homes, were hacked and publicly posted as a result of the company's allegedly lax security practices.[23]

In another case, the FTC was concerned that a rent-to-own company helped its franchisees install and use privacy-invasive software on laptops that consumers rented.[24] The main purpose of this software was to allow franchisees to disable a computer remotely if the consumer fell behind on her payments. However, it also had a "Detective Mode," which allowed franchisees surreptitiously to activate the computer's webcam. As the Commission alleged in its court papers, "[w]ebcams operating secretly inside computer users' homes took photographs of computer users and anyone else within view of the camera."[25] The Commission made clear that collecting such sensitive images in this manner was a source of "actual consumer harm"[26] and unfair.

Homes are sensitive areas, and family life is something that those of us who are not on reality TV shows regard as deeply personal. But there are other kinds of data that are sensitive.

Health information, financial information, and information about children, for example, are also highly sensitive. The law protects these categories information through laws enacted a long time ago – some when I was in grammar school.[27] These protections are based on data flows and business models that made sense when the relevant laws were enacted. They make less sense today. For example, the federal health data protection law, known as HIPAA, was passed at a time when doctors, hospitals, insurance companies, and a handful of entities handled

---

[21] Hewlett-Packard, *Internet of Things Research Study* 2 (July 2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

[22] TRENDNet, Inc., No. C-4426 (F.T.C. Feb. 7, 2014), at ¶ 8 (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[23] *Id.* at ¶¶ 9-11.

[24] *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.

[25] Aaron's, Inc., Case No. 4442 (F.T.C. Mar. 10, 2014), at ¶ 5 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/140311aaronscmpt.pdf.

[26] *Id.* ¶ 16.

[27] *See, e.g.*, Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 *et seq.*; Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No.104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809.

personal health information. And the law applies to them. These days, anyone from the vendor of a fitness app, to a social network, to a marketer that you've never heard of can have detailed information about your health. It's very unlikely that any of these entities are subject to HIPAA.

The Internet of Things will make it easier to measure or infer these kind of data, and big data analytics will improve companies' ability to make sense of the data and use it. Big data has many potential benefits, but I also see a clear potential for this data to be used in surprising and harmful ways. This brings me to the second major privacy challenge of the coming years, relating to big data, fairness and discrimination.

Big Data, Privacy, and Fairness

Basic principles can take us a long way in thinking about how to protect individual privacy and data security, even as technologies make tremendous leaps in terms of how pervasive they and how much data they scoop up. Many of the bedrock privacy principles that we still use today – tell consumers what data you're collecting, give them appropriate choices over how data is used, don't collect data that you don't need – were created in an era of mainframe computers that were the province of a few large corporations and government agencies.[28] These principles have served us well.

But there are some emerging areas where the basic principles are incomplete or it isn't clear how to operationalize them. The questions in these areas go beyond privacy to encompass broader questions of fairness. Companies are reaching further for data that could shed light on individual traits and characteristics. Much of this individual-level analysis is done in the context of "marketing," but that label underplays some of what's at stake. For example, in the FTC's May 2014 report on data brokers, we detailed how the vast amounts of data that are available about each of us can be used to create alarmingly detailed profiles.[29] These profiles can tell marketers a great deal about where we live, where we work, how much we earn – as well as our daily activities (both offline and online), and our interests. But they can also contain inferences about more sensitive attributes, such our race, our health conditions, and our financial status. Data brokers may describe us as "Financially Challenged" or perhaps having a "Bible Lifestyle."[30] They may place us in a category of "Diabetes Interest" or "Smoker in Household."[31] Some of them sell marketing lists that identify consumers with addictions or AIDS. Others focus on ethnicity and finances, creating consumer lists such as "Metro Parents" (which are lists of single parents who are "primarily high school or vocationally educated" and are handling the "stresses of urban life on a small budget") and "Timeless Traditions" (a list of immigrants who "speak[] some English, but generally prefer[] Spanish").[32]

[28] *See* IOT REPORT, *supra* note 15, at 19-20 (discussing history of privacy principle statements).

[29] *See* FTC, DATA BROKER REPORT, *supra* note 13, at 1 (defining "data broker").

[30] *Id.* at 20 n.52, 21.

[31] *Id.* at 46, 55.

[32] *Id.* at 20 n.52.

Marketing based on such profiles could benefit consumers. For example, banks might target "Financially Challenged" consumers with offers for safe, low-cost banking products as an alternative to high-cost options like check cashing services and payday loans. But those high-cost lenders could just as easily purchase the same data and use it to target consumers. This is, in some sense, "just marketing," but it involves a combination of precision and financial impact that could harm low-income and other vulnerable consumers by encouraging them to take on high-interest debt that can deepen their financial distress.

The same data that fuels marketing based on individual consumer profiles can also be used for more substantive decisions about consumers. An increasing range of algorithmic scores and decisions are part of so-called "risk mitigation" services and other potentially significant decisions about consumers. These services answer questions like "Is this consumer who she claims to be?" and "Is the purchase that this consumer is attempting to make likely to be fraudulent?" While some uses of these "risk mitigation" scores may fall under existing consumer protection statutes, such as the Fair Credit Reporting Act (FCRA), [33] an important set of them does not.

And with respect to this latter set of circumstances, consumers do not have the right to know when their profiles are being used to reach adverse decisions about them or to dispute and correct inaccurate information in those profiles. In addition, a lot remains unknown about how big data-driven decisions may or may not use factors that are proxies for race, sex, or other traits that U.S. laws generally prohibit from being used in a wide range of commercial decisions.

This spectrum of data-powered decision-making will be driven by the availability of even more data as the Internet of Things and other technologies develop, and it will certainly take advantage of advances in algorithms to make more precise predictions and inferences. What can be done to make sure these products and services –and the companies that use them – treat consumers fairly and ethically?

I believe that we need to bring more transparency and accountability to the data collection practices that fuel big data analytics, as well as to the uses of analytics. Consumers need a better understanding of what is happing with their data. They should be able to exercise appropriate control over information that goes into the pipelines that feed the algorithms that end up having an effect on their lives, particularly where the pipelines are not visible to consumers. I have long urged data brokers and similar firms to give consumers tools so they can tell companies that they do not want to have their information used for marketing purposes. Consumers should also have the ability to correct information that is used for risk mitigation and other comparably substantive decisions. And these tools should be immersive, with intuitive UIs, so consumers can easily exercise this control. The FTC's data broker report, as well as the White House's big data review, included my recommendations.[34]

---

[33] 15 U.S.C. § 1681 *et seq.*

[34] *See* DATA BROKER REPORT, *supra* note 13, at 49-54; EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES (May 2014), *available at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

Some in industry are taking steps to provide greater transparency and control to consumers, but we have a very long way to go here. Ultimately, I believe we need legislation to address these issues, but industry can and should do more right now to make these tools available to consumers.

Privacy and Data Security in a Global Digital Economy

Now let me turn to the global arena. The Internet of Things, big data analytics, and the other dimensions of our data-intensive economy are all unfolding in a global economy. If you go out and practice privacy and data security law – even if you don't end up focusing on international issues – you will probably run into challenges involving different national privacy laws from time to time.

In fact, international issues will only become more important over time. You have heard that the revelations made by former NSA contractor Edward Snowden have rocked transatlantic relations on privacy and other issues for more than two years. You may also be hearing about how privacy is factoring in to various trade agreements. And you might have heard about how "data localization" requirements – which require companies to maintain data centers inside the borders of the relevant country – and discussions over encryption are becoming focal points of debates about the future of the digital economy and just how global it will be. These issues intersect, legally and economically, with what many U.S. companies do on a daily basis. Some fluency in global issues will be an asset to those of you who are thinking about becoming privacy lawyers.

One thing that you might hear from your international colleagues is that the United States has no privacy law and that it is the "Wild West" when it comes to data protection. This is a myth, and I spend a lot of time in Europe and elsewhere trying to dispel it. The FTC not only protects consumer privacy by enforcing the FTC Act, but we also enforce a number of sector-specific privacy laws. These include the FCRA, the Children's Online Privacy Protection Act (COPPA),[35] which applies to children under 13; and the Gramm-Leach-Bliley Act, which sets privacy and security requirements for financial institutions.[36] Other federal agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, and the Department of Health and Human Services, play an important role in enforcing data protections in the sectors that they oversee. States also enforce consumer privacy protections and are increasingly active in enacting privacy and data security legislation. And, where government surveillance is concerned, we have protections under the Fourth Amendment as well as multiple statutes.

This system of privacy protections is strong, though it can and should be stronger. Its protections are tuned to meet the realities of specific economic activities and provide stronger protections for sensitive information. At the same time, it provides flexibility for companies that are creating new products and services. But one thing that the system of U.S. privacy laws

[35] 15 U.S.C. §§6501-6506.

[36] 15 U.S.C. §§6801-6809.

doesn't do is allow us to point to one law as a means of demonstrating to colleagues in other countries that the United States takes data protection seriously.

The situation is different in many other countries. Europe has a comprehensive Data Protection Directive, which applies to all 28 Member States. Mexico, Israel, Japan, Singapore, and other countries also have a baseline privacy law in place.

These differences have real economic consequences. The EU's Data Protection Directive prohibits companies from transferring personal data out of the EU, unless the destination has a privacy law that offers "adequate" protections, with "adequacy" determined by the European's administrative body, known as the European Commission. The United States does not have one of the adequacy findings, and indeed the U.S. government has never sought adequacy. Shortly after the Directive went into force, the U.S. government recognized that the adequacy requirement put around $120 billion in annual trade at risk. And that was in the year 2000.

Cutting off this trade wasn't in the interest of the U.S. or Europe, and this mutual interest in transatlantic data flows led to the U.S.-EU Safe Harbor Framework. Safe Harbor allows individual companies to certify that they provide adequate protections for personal data. Safe Harbor has two main pieces. First, it spells out seven privacy principles that companies must follow, such as notice, choice, access, and security. Second, the Safe Harbor Framework says that companies must certify and publicly declare that they follow the Safe Harbor principles in their own data practices. The FTC plays an essential role in the Safe Harbor Framework, because it is the agency that enforces companies' commitments to abide by its principles.

For more than a decade, Safe Harbor was a fixture of the transatlantic economy. Then, in June 2013, the Snowden disclosures revealed the U.S. intelligence agencies had developed very extensive capabilities to collect digital information for foreign intelligence purposes. National security and foreign relations are not part of the FTC's mission, nor are there intelligence or law enforcement requirements in the Safe Harbor Framework.

Nonetheless, the Safe Harbor Framework has been a focal point of European officials' and advocates' scrutiny for the past two years. At the end of 2013, the European Commission demanded 13 changes to the Framework,[37] and the Department of Commerce has been negotiating these changes ever since. The FTC has worked closely with the Department of Commerce, supporting many of the EC's recommendations because they made good sense and would improve protections for consumers in the U.S. and Europe. I am hopeful that this negotiation will wrap up soon, and many signs are pointing in this direction.

But the Safe Harbor negotiation may end up being just one scene in a much longer play. The European Court of Justice, which is analogous to a Supreme Court for the European Union, is currently considering a more fundamental legal challenge to the Safe Harbor Framework, again based on the Snowden revelations. The European Union is also close to finalizing a

[37] *See* European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (Nov. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

General Data Protection Regulation to replace the current Directive.[38] It remains to be seen exactly how existing adequacy arrangements, such as Safe Harbor, will be treated both by the European Court of Justice and under the new Regulation.

And these are just some of the known unknowns. Other developments, like the Right to be Forgotten, are still unfolding and will also raise new questions for consumers as well as companies that operate globally. And I'm sure there will be many other surprises, both good and bad, in the years ahead.

* * * * * *

Despite this uncertainty, I'm optimistic that the U.S., Europe, and other regions will keep moving toward more ways for companies to do business globally while providing strong, consistent, and enforceable privacy protections. The economic case for free global data flows is compelling, and this is something that nearly all governments recognize. At the same time, I fervently believe that privacy is a fundamental value that we need to protect, and many of my counterparts in other government agencies and other countries share this view. Far from being a clash between irreconcilable values, privacy and the development of a data-intensive economy should be mutually reinforcing goals. But success in building privacy and security into the Internet of Things, big data analytics, and other new uses of technology is a big project that requires constant efforts by advocates, industry, academics, and the government. I urge you to consider joining the effort.

Thank you.

[38] *See* Remarks by Commissioner Jourová After the Launch of the Data Protection Regulation Trilogue (June 24, 2015), *available at* http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm (outlining main issues that remain under discussion in connection with the Regulation).