Global Regulation of Data Flows in a Post-Snowden World
Tuck School of Business
Dartmouth College
February 18, 2015

Good afternoon. Thank you, Matthew, for your kind introduction, and congratulations on being named Dean of the Tuck School. And I very much appreciate the Center for Global Business and Government's invitation to speak here today. It is a pleasure to speak with you, the next generation of business leaders and the faculty members who are getting them ready to assume this role.

The Internet has become today's global trade route.[1] The Internet has made it not only possible but easy for companies to deliver products and services to consumers all over the world. One study found that economic activity taking place over the Internet is growing at 10% per year within the G-20 group of nations.[2] The Department of Commerce reported last year that the U.S. exported nearly $360 billion in digitally deliverable services, and that the national surplus in such services is about $135 billion.[3]

One of the key drivers in the Internet economy is the flow of personal data. In the context of online services, the collection and analysis of data about individual consumers is integral to how some of the largest companies in the world do business. For example, Facebook has become a company with a $200 billion capitalization largely through its sales of ads that reach Facebook users.[4] But data also allows small and medium companies to monetize their services. The World Economic Forum believes that data driven enterprise could be part of a strategy for economic development in vulnerable regions of the world.[5]

At the same time, we are seeing the development of a new wave of innovations based on connecting everyday objects – from light bulbs to appliances to cars – to the Internet. This phenomenon, known as the Internet of Things, promises not only to make our lives more convenient and efficient but also to offer insights that could help us solve some of society's most pressing problems. This is due not only to connected devices themselves but also to the data that they generate. Data from wearable fitness devices could help each of us get motivated to eat better or exercise more, while also providing important information to health researchers. Data

---

[1] William E. Kennard, U.S. Ambassador to the EU, Winning the Future Through Innovation, Remarks Before the AmCham EU Transatlantic Conference (Mar. 3, 2011), *available at* http://useu.usmission.gov/kennard_amchameu_030311.html.

[2] World Econ. Forum, DELIVERING DIGITAL INFRASTRUCTURE: ADVANCING THE INTERNET ECONOMY 7 (Apr. 2014), *available at* http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf.

[3] Dept. of Commerce, Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services 2 (Jan. 2014), *available at* http://www.esa.doc.gov/sites/default/files/digitaleconomyandcross-bordertrade.pdf. [DIGITAL CROSS BORDER TRADE REPORT]

[4] *See* YCharts, Facebook Market Cap (Feb. 13, 2015), http://ycharts.com/companies/FB/market_cap.

[5] *See generally* World Economic Forum, DATA-DRIVEN DEVELOPMENT: PATHWAYS FOR PROGRESS (Jan. 2015), *available at* http://www3.weforum.org/docs/WEFUSA_DataDrivenDevelopment_Report2015.pdf.

from connected cars might help us find a quicker route to our destination, and shed light on how traffic engineers should design highways to minimize traffic delays. And when teachers use tablets and apps in their classrooms, they can expose their students to challenges and experiences that are individually tailored while, at the same time, giving educators and researchers greater insight into what works – and doesn't work – in education.

So a great deal rides on data – and not just any kind of data, but *personal* data. This means that a great deal also rides on how we protect this personal data. Protecting individual privacy and keeping data secure are integral to the success of the data-driven economy because they are essential to earning and keeping consumers' trust. I spend a lot of time talking with industry leaders from many sectors of the economy, and they understand this. Put simply, none of them wants their company to be in the headlines for failing to implement reasonable data security, deceiving consumers about the company's data practices, or collecting or using consumers' data unfairly.

But engendering consumer trust in the data-driven economy isn't as simple as companies' compliance with federal and state laws. Because data flows are now global, so are data privacy and security issues. Here in the U.S., protecting consumer privacy and data security are top priorities at the Federal Trade Commission and other state and federal agencies, and I am proud of the work we do along these lines. But I'll be honest with you: the U.S. privacy framework is different from those in Europe, Asia, and Latin America. While the United States embraces many of the same privacy principles as other countries, and we have developed ways to make our systems interoperable, the differences also create real challenges.

The first challenge is that some international thought leaders – within the government, business community and civil society of our trading partners – do not fully understand U.S. privacy law. Some of them believe that our system offers little or no privacy or security protections for data about individuals. Some say that the U.S. is the "Wild West" where data practices are concerned. Others think that privacy protections in the U.S. are voluntary, and the only way that a company can get into trouble is by making a promise about a product or service that it offers, and then failing to live up to that promise. I would like to explain why these notions are misunderstandings. In the process, I hope to give you a better sense of what U.S. law requires – and what the Federal Trade Commission expects – of companies under its jurisdiction.

The second challenge is for those of you who end up working at a data-driven firm with global reach – and this description now fits car companies, appliance manufacturers, and many other firms, in addition to traditional "Internet" companies. You will need to navigate different national privacy laws and the cultural and political systems in which they're embedded. How the privacy laws in other countries relate to our own is the subject of intense debate, particularly in Europe in the wake of revelations about the U.S. intelligence community's data collection activities. While I can't offer tidy predictions about how these debates will be resolved, or when, I can give you reasons to be optimistic that things will work out.

The U.S. Consumer Privacy Framework: Different But Comprehensive

The notion that the United States doesn't have a privacy law stems primarily from the fact that we do not have a single, comprehensive law that governs the collection, use, and disclosure of personal information in the commercial sphere. Instead, here in the U.S. there are a variety of federal and state laws that play an important role in protecting the privacy and security of individuals' information. Some federal privacy laws apply to specific sectors, such as healthcare,[6] banking,[7] credit reporting,[8] and communications.[9] Other federal laws protect children's and students' privacy.[10] The states have many additional privacy laws that range from limiting employers' ability to view their employees social network accounts,[11] prohibiting employers and insurers from using information about certain medical conditions,[12] and requiring online services to allow minors to delete information they have posted[13] – to requiring companies to notify consumers when they suffer a security breach involving personal information.[14] In addition to these specific laws, Section 5 of the Federal Trade Commission Act[15] prohibits "unfair or deceptive acts or practices,"[16] and the FTC has used this authority to address a number of data security and privacy practices that fall through some of the gaps in more specific laws.

The FTC has been a cop on the privacy and data security beat since the rise of the commercial Internet. The FTC entered this arena because the potential for consumers to be harmed by losing control of personal information was clear. Over the past 15 years or so, we have brought nearly 100 actions 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

---

[6] 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.).

[7] 15 U.S.C. §§ 6801-09.

[8] 15 U.S.C. § 1681 *et seq.*

[9] 47 U.S.C. §§ 222, 338, and 631.

[10] *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06; Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

[11] *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).

[12] *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).

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

[14] *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).

[15] 15 U.S.C. § 45.

[16] 15 U.S.C. § 45(a).

Snapchat.[17] We have also brought cases against companies that are not household names, but violated the law by spamming consumers,[18] installing spyware on their computers,[19] failing to secure consumers' personal information,[20] deceptively tracking consumers online,[21] violating children's privacy,[22] and inappropriately collecting information on consumers' mobile devices.[23] 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. I'd like to spend a moment or two explaining how my agency has done this.

FTC Enforcement of Companies' Unfair and Deceptive Collection and Use of Sensitive Information

First, let's consider some of the Commission's actions against companies for failing to provide appropriate transparency and choice about their personal data practices to consumers. Many of our cases in this arena have been pretty straightforward: a company *said* it would do one thing, but it actually *did* something else.[24]

---

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

[18] *See, e.g.*, FTC v. Flora, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf.

[19] *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* http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf.

[20] *See* FTC v. Bayview Solutions, LLC, Case 1:14-cv-01830-RC (D.D.C. Aug. 27, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf *and* FTC v. Cornerstone and Co., LLC, Case 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf. The courts in both cases have entered preliminary injunctions against the defendants.

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

[22] *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* http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf.

[23] *See* United States v. Path, Inc., No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (consent decree and order), *available at* http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf; HTC America, Inc., C-4406 (F.T.C. June 25, 2013) (decision and order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf.

[24] *See, e.g.*, *In re GeoCities, Inc.*, 127 F.T.C. 94 (1999) (consent order) (settling charges that website had misrepresented the purposes for which it was collecting personally identifiable information from children and adults); *FTC v. Toysmart.com, LLC*, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (consent order) (challenging website's attempts to sell children's personal information, despite a promise in its privacy policy that such information would never be disclosed).

Things get more interesting when a company provides some information about their data collection and use practices to consumers, but leaves out material information about other practices. To take one example, in March 2014, the FTC brought an action against the vendor of an app that turned the LED on a mobile phone – most widely known for turning into a flash bulb for the phone's camera – into a flashlight. But we believed the flashlight app was collecting precise geolocation information, along with a number that uniquely identified consumers' phones. The company's privacy policy disclosed that the app collected data for product support and similar purposes, but inappropriately failed to mention the collection of this more sensitive information.[25]

The FTC has also used Section 5 to address data collection irrespective of specific representations to consumers. In 2013, for example, the FTC brought an action against a firm that developed software for rent to own companies to install on computers they offered to consumers, to disable the computer if the consumer failed to make timely payments, or the computer was stolen. An add-on feature for the software, called "Detective Mode", allowed the rent-to-own companies to log keystrokes and capture screenshots of confidential and personal information such as user names and passwords, social media interactions and transactions with financial institutions. It also allowed the rent to own companies to take pictures of anyone within view of the computer's webcam, all without even alerting consumers to the existence of the software.[26] We believed that collecting this deeply personal information was harmful to consumers, and therefore unfair.[27]

To protect privacy comprehensively, we need to address more than just how companies collect and use personal information. Companies also need to ensure that they don't engage in practices that enable others to inappropriately obtain personal data through breaches or hacks. The FTC plays an important role in ensuring companies are employing reasonable data security practices to prevent harm to consumers from data breaches. Data security is a large part of our enforcement program. Over the past 13 years, we have brought 55 cases involving companies that we believed failed to engage in reasonable data security practices. The FTC's initial data security enforcement efforts focused on the financial harms that consumers could suffer when their Social Security numbers or information about their credit cards or bank accounts fell into the wrong hands.[28] But we also focus on security lapses that expose other types of sensitive

---

[25] Goldenshores Techs., LLC, C-4466 (F.T.C. Mar. 31, 2014) ¶¶ 11-12 (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf.

[26] DesignerWare, LLC, C-4390 (F.T.C. Apr. 11, 2013), at ¶ 14 (complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf . The Commission also settled an action against the rent-to-own company that used the software and its franchisees.

[27] An unfair act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

[28] *See, e.g.*, The TJX Cos., Inc., No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter; Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; DSW, Inc., No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; *BJ's Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

personal information,[29] including medical information,[30] pharmaceutical records,[31] and our social contacts.[32]

We also examine data security practices even where companies have not suffered from a security breach. Last year, for example, we settled actions with Credit Karma and Fandango for releasing mobile apps that were allegedly vulnerable to a well-known attack that could have led to the interception of credit card numbers, Social Security numbers, and other sensitive personal information that the apps transmitted.[33]

I believe that privacy and security are two sides of the same coin, because you cannot have privacy if your information is not secure. Some of our recent cases demonstrate this fact, showing that data security is an integral part of privacy. In our first enforcement action involving the Internet of Things case, we alleged that the defendant company's Internet-connected cameras were vulnerable to having their feeds hijacked.[34] 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.[35] And in our enforcement action involving Snapchat, we alleged that the company deceived consumers in a number of ways about privacy and security. The part of the FTC's complaint that seemed to draw the most attention was the allegation that recipients of video or photo "snaps" could save them indefinitely using a few simple techniques, despite the company's representation that snaps would "disappear forever" after a short period of time.[36]

---

[29] *See* HTC America, Inc., C-4406 (F.T.C. June 25, 2013) (decision and order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf.

[30] *See* GMR Transcription Servs., No. C-4482 (F.T.C. Aug.14, 2014) (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf.

[31] *See* FTC, Press Release, Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (July 27, 2010), *available at* http://www.ftc.gov/news-events/press-releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-and; FTC, Press Release, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), *available at* http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial.

[32] *See* Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), at ¶¶ 34-45 (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

[33] FTC, Press Release, Fandango, Credit Karma Settle FTC Charges That They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

[34] 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.

[35] *Id.* at ¶¶ 9-11.

[36] Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), at ¶¶ 6-19 (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

But we also alleged that the app exposed consumers' mobile phone numbers,[37] and left consumers vulnerable to being impersonated by other Snapchat users.[38]

From time to time, I discuss these issues with my data protection colleagues in other countries – describing the scope and nuances of our privacy and data security laws in the U.S., as well as the breadth of our enforcement work. These conversations, and others like them, have helped increase the understanding abroad that, far from being the Wild West of data collection and use, the U.S. (and particularly the FTC) engages in robust and careful privacy enforcement, including against companies whose data practices cause substantial harm, even if the companies make no promises about how they collect, use, or share data.

Strengthening the U.S. Privacy and Data Security Framework

While Section 5 and sector-specific data privacy laws create good protections for consumers and their data, I believe our consumer privacy and data security framework can and should be improved. As more and more sensitive information flows throughout the commercial marketplace, I think it is important to ensure that the data are appropriately protected. For example, health and personal financial information are at the center of many new apps, services, and devices – and many of them are operated by companies that are not covered by our sector specific laws governing health and financial information. Yet the information is just as sensitive and deserving of protection.

The growth of the Internet of Things, while exciting, will increase the need to adapt our data security laws. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.[39] A recent study by Hewlett-Packard found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[40] And the data security concerns raised by connected devices involve not only unauthorized access to personal information, but also involve security threats to device functionality itself. If a device like a pacemaker[41] or a car[42] is hacked, very sensitive information could be compromised and the person using the device could be seriously harmed.

---

[37] *Id.* at ¶¶ 30-33.

[38] *Id.* at ¶¶ 34-45.

[39] 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.

[40] 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.

[41] *See* Barnaby Feder, *A Heart Device Is Found Vulnerable to Hacker Attacks*, N.Y. TIMES (Mar. 12, 2008), *available at* http://www.nytimes.com/2008/03/12/business/12heart-web.html.

[42] *See* Dan Goodin, *Senator: Car Hacks That Control Steering or Steal Driver Data Are Way Too Easy*, ARSTECHNICA (Feb. 9, 2015 4:02 PM), *available at* http://arstechnica.com/security/2015/02/senator-car-hacks-that-control-steering-or-steal-driver-data-way-too-easy/.

Finally, consumers need to know more about and have better protections from inappropriate uses of data behind the scenes. Data brokers are companies that assemble individual profiles on consumers by collecting information from far-flung sources, but typically do not interact with consumers themselves. Through these profiles, consumers can end up in marketing segments drawn along lines of race, ethnicity, financial status, health conditions, and other sensitive characteristics. Consumers deserve much more transparency and control concerning these profiles and their uses. And as *all* companies begin to mine their own data for insights – Who are our best customers? Who is a high (or low) priority for customer service? – they also need to avoid treating their own customers in a manner that is unfair or discriminatory.

Common sense steps have been proposed to deal with many of these concerns. President Obama visited the FTC just last month and, while there, called on Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen the FTC's existing data security enforcement tools, and to provide notification to consumers when there is a security breach.[43] The President also announced that he would seek to introduce baseline privacy legislation that would create clearer rules of the road and give the FTC stronger enforcement tools, like the authority to obtain civil penalties from companies that break the law. The FTC has supported legislation on both fronts.[44] In addition, both the White House[45] and the FTC[46] have called for data broker legislation that would bring more transparency and give consumers more choices about their data that is collected and used by data brokers.

That's an ambitious agenda. While we work with Congress to develop these legislative solutions, the FTC will continue to encourage companies to implement some of these reforms through best practices.[47] And the FTC will continue to use its authority under Section 5 and sector-specific laws to protect privacy and data security in the United States. Although it is not perfect, Section 5 allows us to proceed against a wide range of harmful data practices and

---

[43] President Barack Obama, Remarks at the Federal Trade Commission (Jan. 12, 2015), *available at* http://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

[44] *Id.*

[45] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[46] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 49-54 (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [DATA BROKER REPORT].

[47] *See, e.g.*, FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 29-46 (staff report) (2015), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (recommending best practices regarding data security, data minimization, and notice and choice on connected devices and associated services); DATA BROKER REPORT, *supra* note 46, at 54-56 (recommending that data brokers adopt best practices of privacy by design, accountability, and refraining from collecting information from children and teens); *See* Jared Ho, Comments at Federal Trade Commission Consumer Generated and Controlled Health Data Seminar 26–27 (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf; FTC, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING (Mar. 2013), *available at* http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

provides for strong remedies that protect consumers and improve how companies handle data. This framework is effective, and it is uniquely American.

Handling Differences: Interoperability in a Post-Snowden World

Other countries handle privacy differently. Most countries with industrialized economies have a baseline law that governs data practices in the commercial sphere. This is certainly the case in Europe, as well as Canada, Mexico, Israel, and Japan, to name a few. Some privacy regimes present unique challenges, including the emergence of data localization laws.[48] Yet for the FTC and other parts of the U.S. government, as well as companies that do business globally, Europe presents some of the most urgent questions about privacy frameworks and global data flows, so that's where I'll focus my attention today.

One of the major differences between the U.S. and EU privacy frameworks is that, in Europe, privacy is a fundamental right. The Charter of Fundamental Rights establishes rights to the protection of private life and of personal data.[49] The EU's 1995 Directive[50] adopts a comprehensive set of privacy rights that determine how companies may legally process data about EU citizens. The Directive requires each of the Member States of the EU – all 28 of them – to adopt a national law that implements the principles of the Directive. In the U.S., we have enshrined some privacy principles within the Constitution's Fourth[51] and Fourteenth Amendments,[52] but the privacy and security of consumer information generally has not yet been recognized as a Constitutional right.

Yet I find that the U.S. and EU have a great deal in common when we move beyond this question of rights, and examine the individual liberties and other values that we want to protect, including protecting consumer privacy in a data-driven economy. Issues of trust, including privacy and data security, are a pillar of the ambitious Digital Agenda put forth by the European Commission, which is the administrative arm of the European Union's government.[53] The European Commission stated in a July 2014 Communication that we are "witness[ing] a new

---

[48] *See* Natalya Gulyaeva, Maria Sedykh, and Bret Cohen, *Russia Changes Effective Date of Data Localization Law to September 2015*, CHRONICLE OF DATA PROTECTION (Jan. 2, 2015), *available at* http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/russia-changes-effective-date-of-data-localization-law-to-september-2015/.

[49] Charter of Fundamental Rights of the European Union, arts. 7 & 8, 2000/C 364/01 (2000), *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[50] *See generally* Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and of the Free Movement of Such Data, 95/46/EC (Oct. 24, 1995), *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf ["Data Protection Directive"].

[51] *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).

[52] *See, e.g.*, Loving v. Virginia, 388 U.S. 1 (1967) (holding that a state statute prohibiting interracial marriage violated the Equal Protection and Due Process Clauses of the Fourteenth Amendments).

[53] European Commission, Digital Agenda Scoreboard (last visited Feb. 17, 2015), *available at* http://ec.europa.eu/digital-agenda/en/digital-agenda-scoreboard.

industrial revolution driven by digital data, computation and automation,"[54] and concluded that fully developing this potential requires ensuring that "[u]sers have sufficient trust in the technology, the behaviors of providers, and the rules governing them" and that appropriate data protection laws are ways to build this trust.[55] Similarly, the Article 29 Working Party, which consists of data protection authorities from EU Member States, also noted last September that the Internet of Things holds "significant prospects of growth for a great number of innovating and creative EU companies" but also stated that "these expected benefits must also respect the many privacy and security challenges."[56] These efforts in Europe to tie together the promise of the data-driven economy with the need to appropriately address privacy and security are similar in many ways to the discussions underway here in the U.S., driven by policy recommendations from the White House and from the FTC.

Moreover, just as we have done in the United States, European policy makers have identified gaps and other problems in their own privacy framework, and are seeking to address them. The EU is in the midst of a years-long process to address these challenges through a new privacy law. This new law will be a Regulation, rather than a Directive, meaning that there will be a single law for the entire EU. The proposed Regulation borrows from U.S. law in its efforts to add some protections first developed here, including heightened protections for children's information and notification to consumers after data security breaches. The proposed Regulation also could include enhanced enforcement tools by increasing fines and creating a more streamlined process for the various data protection authorities to engage in investigations and enforcement. The Regulation could also bring greater clarity to issues that are at the center of fervent debate among companies, advocates, and privacy officials, such as the role of consent in data protection and the contours of a "right to be forgotten".

The proposed Regulation is working its way through a complicated legislative process that involves the European Commission, Parliament, and Council. Many observers are predicting that the Regulation will be adopted in 2016, with implementation potentially years later.

For now, the Directive governs. And it includes another important aspect of European privacy law: It prohibits companies from sending EU citizens' data outside the EU unless the destination is a country that provides an "adequate level of protection" for the data.[57] The European Commission has the authority to determine whether non-EU countries meet this adequacy requirement.[58] Several countries have applied for and obtained adequacy.[59] The United States is not among them.

---

[54] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, Towards a Thriving Data-Driven Economy, at 5, July 2, 2014, *available at* https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy.

[55] *Id.* at 11.

[56] Art. 29 Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 3 (Sept. 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[57] Data Protection Directive, *supra* note 50, art. 25(1).

[58] *Id.* art. 25(6).

There are, however, mechanisms that allow personal data to legally flow from the EU to the United States. From the time that the Directive went into force, the EU and the U.S. recognized that prohibiting such data flows would be harmful to the economies on both sides of the Atlantic. As the initial Safe Harbor negotiations approached their conclusion in 2000, the White House noted that the arrangement would protect privacy in accordance with EU law while "prevent[ing] the potential disruption of approximately $120 billion in U.S.-EU trade."[60] The amount at stake has only increased since then.[61] This mutual interest in transatlantic data flows led to the U.S.-EU Safe Harbor Framework, which allows specific companies to certify that they provide adequate protections for personal data.

There are two main pieces to Safe Harbor. First, the Framework spells out seven privacy principles that companies must follow, such as notice, choice, access, and security.[62] Second, the Framework says that companies that want to be in Safe Harbor 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' Safe Harbor commitments.

The viability of the Safe Harbor was seriously threatened starting in June 2013, when information provided by Edward Snowden began to detail some of the data collection activities of the National Security Agency and other intelligence and law enforcement agencies. Many European officials, advocates, and citizens reacted to these revelations with outrage over what was reported.[63] The European Parliament recommending suspending Safe Harbor.[64] The European Commission took a different approach. It issued a report indicating that the Safe Harbor Framework should be retained, but demanding 13 changes.[65]

---

[59] European Commission, Commission Decisions on the Adequacy of the Protection of Data in Third Countries (last updated Dec. 15, 2014), *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[60] White House, Fact Sheet: Data Privacy Accord with EU (Safe Harbor) (May 31, 2000), *available at* http://clinton4.nara.gov/WH/New/Europe-0005/factsheets/data-privacy-accord-with-eu.html.

[61] *See* DIGITAL CROSS-BORDER TRADE REPORT, *supra* note 3, at 10 (Table 1) (showing consistent increase in digitally deliverable services as a fraction of total U.S. exports from 2002 through 2011).

[62] Dept. of Commerce, Safe Harbor Principles, *available at* http://export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 30, 2009, 3:03 PM) ["Safe Harbor Principles"].

[63] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 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 (Feb. 21, 2014), at ¶ 131 (action 2), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2014-0139&language=EN ["EP Resolution"].

[64] *See id.* at ¶¶ A-K (setting forth concerns raised by U.S. surveillance revelations).

[65] European Commission, Communication on the Functioning of the Safe Harbor from the Perspectives 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.

For more than a year, the Department of Commerce and the European Commission have been negotiating these changes. Many of the items on the European Commission's list are reforms that make good sense and would improve Safe Harbor from a consumer protection standpoint. These changes include eliminating the fees that some EU consumers have to pay to have Safe Harbor-related disputes resolved, increasing transparency in the administration of the Safe Harbor program, and increasing accountability within companies that are in Safe Harbor.[66] Two of the EC's recommendations for improving Safe Harbor concern national security issues.[67] The current Safe Harbor Framework,[68] as well as other mechanisms governing data transfers in the commercial sphere (such as binding corporate rules), and even the EU Data Protection Directive itself, all include exceptions for national security and law enforcement.

The Snowden revelations began a robust conversation on both sides of the Atlantic about whether we have struck the right balance in the law enforcement and national security arenas. The Charlie Hebdo and Jewish market attacks have added some important new perspectives to this discussion in Europe.[69] The conversation on both sides of the Atlantic is critically important, but in my view it should be distinct from the issues surrounding companies' collection and use of consumer data.

In the context of companies' collection and use of consumer data, I believe that Safe Harbor gives the FTC an effective tool to protect the privacy of consumers in the EU and the U.S. As such, Safe Harbor is a solution, not a problem. The FTC has settled 24 actions against companies that allegedly either falsely stated that they were in Safe Harbor but actually were not, or claimed to meet Safe Harbor's substantive requirements but did not.[70] In addition, in November, the FTC announced a settlement with TRUSTe, which maintains a Safe Harbor certification program, over its alleged misrepresentations about the extent to which it conducted annual recertifications for Safe Harbor and other privacy programs.[71]

---

[66] *See* Julie Brill, At the Crossroads 7-8 (Dec. 11, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/crossroads-keynote-address-iapp-europe-data-protection-congress/131211iappkeynote.pdf.

[67] *See* European Commission, Restoring Trust in EU-US Data Flows – Frequently Asked Questions (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

[68] *See* Safe Harbor Principles, *supra* note 62 ("Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; . . .").

[69] *See, e.g.*, Kevin Johnson, *Security vs. Privacy: France Trying to "Find the Line"*, USA TODAY (Feb. 9, 2015 6:54 PM), *available at* http://www.usatoday.com/story/news/nation/2015/02/09/france-terror-surveillance/23118939/.

[70] *See* FTC, Privacy & Security Update (2014), *available at* http://www.ftc.gov/reports/privacy-data-security-update-2014 (noting that "[s]ince 2009 the FTC has used Section 5 to bring 24 Safe Harbor cases").

[71] True Ultimate Standards Everywhere (TRUSTe), FTC Matter No. 1323219, Complaint at ¶¶ 11-16 (Nov. 17, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141117trustecmpt.pdf. Under the FTC's proposed order, TRUSTe is prohibited from making such representations and would be subject to civil penalties if it fails to abide by these terms. *See* TRUSTe, FTC Matter No. 1323219 at § I (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/141117trusteagree.pdf.

* * * *

Where do things go from here? As business leaders and business students, you should probably think about this question the same way you think about mid-February in New Hampshire: we've put a lot behind us, but there's still a long way to go. In terms of the discussions with our European colleagues, I am optimistic about resolving the tensions that have understandably arisen since June 2013. Part of my optimism goes back to the common privacy principles that we share, and the efforts underway on both sides of the Atlantic to examine whether our different privacy frameworks are able to sufficiently protect consumers in an era of big data and the Internet of Things.

Going forward, the appropriate measure of progress should not be which system "wins" [as I was recently asked during a talk in Brussels]. Instead, the appropriate measure is whether the United States and Europe develop practical, effective, and interoperable frameworks that will allow data to be adequately protected and to flow between our economies. Neither the U.S. nor Europe will succeed without getting privacy and data security right, as they are key elements to engendering consumer trust. Consumers – and businesses – need and deserve nothing less.

Thank you.