One Year Later: Privacy and Data Security in a World of Big Data, the Internet of Things, and Global Data Flows

Keynote Address Before the USCIB/BIAC/OECD Conference on "Promoting Inclusive Growth in the Digital Economy"

Commissioner Julie Brill
March 10, 2015

Thank you, Peter, for your kind introduction. And thanks to USCIB, BIAC, and the OECD for inviting me to speak with you. Privacy and data security in the global, data-driven economy are among the most important issues facing companies, consumers, policymakers, and other stakeholders. It is a pleasure to be able to discuss these issues with you this morning.

I was honored to give a keynote speech at this important event last year. When I glanced back at those remarks to prepare for this morning,[1] I was stunned at how much has happened since then. Of course, the Internet is still today's global trade route.[2] Hundreds of billions of dollars of annual international trade continue to be directly tied to data flows between the United States and other countries.[3] And privacy and data security continue to be among the top consumer protection priorities of my agency, the Federal Trade Commission,

But what has changed over the past year is the deep dive we have all taken into the data driven economy, in an effort to figure out how to best protect consumers' privacy and data security, and allow innovation to flourish, as new business models and technologies develop. Over the past year, the FTC grappled with the Internet of Things;[4] and the data broker ecosystem, issuing seminal reports in each of these areas.[5] We also hosted public seminars on cutting-edge issues like user generated health information;[6] retail mobile location tracking;[7] and

---

[1] Julie Brill, Commissioner, Keynote Address at the USCIB/BIAC/OECD Conference on Growth, Jobs & Prosperity in the Digital Age: OECD Shapes the Policy Environment (Mar. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/204981/140310oecd.pdf.

[2] *See* 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.

[3] *See* 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 (reporting that the United States exported nearly $360 billion in digitally deliverable services in 2011).

[4] 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 [IOT REPORT].

[5] 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.

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

scoring individuals based on where they live, their social media interactions, and other nontraditional scoring techniques.[8] And we brought several important enforcement actions dealing with privacy and security of mobile apps and the sensitive personal information that they handle;[9] the security of consumers' health information;[10] and privacy and security in the Internet of Things.[11]

On today's broader theme of promoting inclusive growth in the digital economy, we have examined how big data can serve as a tool of inclusion and a tool of exclusion,[12] and we have issued reports and taken enforcement actions to help ensure that mobile payment systems follow fundamental consumer protection rules.[13]

The Obama Administration also took some big steps in privacy and data security policy over the past year. In May, the Administration released a landmark report on big data's economic and social opportunities, as well as its challenges to privacy, fairness, and other fundamental values.[14] The Administration also renewed its call for breach notification legislation,[15] called for new federal student privacy legislation,[16] and, most recently, outlined its

---

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

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

[9] *See, e.g.*, Snapchat, Inc., No. 4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf; Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmado.pdf; Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf.

[10] *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 (alleging that the respondents failed to maintain reasonable data security through their alleged failure to require a third-party contractor to maintain reasonable security, among other things).

[11] *See* TRENDnet Inc., No. C-4426, 2014 WL 556262 (F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

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

[13] *See* FTC, WHAT'S THE DEAL? AN FTC STUDY ON MOBILE SHOPPING APPS (Aug. 2014), *available at* https://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf; FTC, PAPER, PLASTIC OR . . . MOBILE? AN FTC WORKSHOP ON MOBILE PAYMENTS (Mar. 2013), *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion; Google, Inc., No. C-4499 (F.T.C. Dec. 2, 2014) (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/141205googleplaydo.pdf; Apple Inc., No. C-4444 (F.T.C. Mar. 25, 2014) (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/140327appledo.pdf.

[14] EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

[15] *See* The Personal Data Notification & Protection Act, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (last visited Mar. 9, 2015).

views on baseline privacy legislation in the form a discussion draft of the Consumer Privacy Bill of Rights.[17]

But that's not all. In Europe, the effort to pass a general data protection Regulation moved forward. The European Parliament passed its version of the Regulation,[18] and the European Council released some of its agreed to provisions.[19] The U.S. and the European Commission continued to discuss changes to the Safe Harbor Framework.[20] The Court of Justice for the European Union ruled that Europeans' fundamental right of privacy includes a right to be "forgotten."[21] And just to demonstrate that the discussion about data flows and privacy is truly global, Brazil[22] and Japan[23] are among the other countries that are in the midst of revising or adopting data privacy laws.

While technologies and business models change rapidly, many developments of the past year have confirmed one important message: basic consumer protection principles apply to exciting new technologies, and we need to keep consumers front and center as we develop policies for privacy and security in our increasingly connected world.

Internet of Things and Big Data

The Internet of Things illustrates this point well. The data that we collect from the Internet of Things could help solve some of society's big challenges in healthcare, energy,

---

[16] *See* 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 (announcing proposal of Student Digital Privacy Act).

[17] Administration Discussion Draft – Consumer Privacy Bill of Rights Act of 2015, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (last visited Mar. 9, 2015).

[18] European Parliament, Legislative Resolution of 12 March 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (last visited Mar. 9, 2015).

[19] See Cynthia O'Donoghue, EU Council Agrees on Partial General Approach to General Data Protection Regulation, Global Regulatory Enforcement Law Blog (Dec. 18, 2014), available at http://www.globalregulatoryenforcementlawblog.com/2014/12/articles/data-security/eu-council-agrees-on-partial-general-approach-to-general-data-protection-regulation/.

[20] *See infra* note 35 and accompanying text.

[21] *See generally* Google Spain SL v. Agencia Española de Proteccíon de Datos ¶ 14, (Court of Justice of the European Union, Case C 131/12), *available at* http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL.

[22] *See* Hunton & Williams, *Brazil Releases Draft Personal Data Protection Bill*, PRIVACY AND SECURITY LAW BLOG (Feb. 6, 2015), *available at* https://www.huntonprivacyblog.com/2015/02/articles/brazil-releases-draft-personal-data-protection-bill/.

[23] *See* Jones Day, Framework for Amendment to Japan's Personal Information Protection Act (Aug. 2014), *available at* http://www.jonesday.com/Framework-for-Amendment-to-Japans-Personal-Information-Protection-Act-08-28-2014/?RSS=true.

education, transportation, and other key areas. But much of the data that comes from sensors in our homes and on our bodies will be deeply personal, and say a great deal about us as individuals. At the same time, as Eric Schmidt said recently, "the Internet will disappear."[24] Just as you forget about shifting gears in your car once you have an automatic transmission, connectivity will just be part of the way things work. So, many of the cues that we rely on to know when we're connecting to a network or sending information may soon vanish. But the need to protect consumers' data will not.

Security is paramount in the Internet of Things. To give you a sense of where things are at the moment, 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.[25] Moreover, traditional consumer goods manufacturers are entering the Internet of Things market and may not have spent decades thinking about how to secure their products and services from hackers in the way that traditional technology firms have. And many connected devices will be inexpensive and essentially disposable. If a vulnerability is discovered on such a device, will manufacturers notify consumers, let alone patch the vulnerability?[26] And *device* security will be just as important as *data* security, to ensure that the functionality of connected cars, pacemakers and other devices are reasonably protected.[27] Our report offers some solid practical advice on security of connected devices.[28]

Data minimization also plays a key role in promoting data security and privacy. You can't lose or misuse what you don't have. For that reason, the FTC has long pushed companies to practice data minimization.[29] We renewed this call in our report on the Internet of Things, suggesting that companies limit the consumer data they collect and maintain to the information they truly need, and dispose of the information once they no longer need it.[30] We also call on companies to deidentify the data they do keep. From the FTC's perspective, effective deidentification combines reasonable technical deidentification with accountability measures that prohibit the company that controls the data from attempting to reidentify it, and places the same prohibitions on any recipients of the deidentified data.[31]

Finally, the need for consumers to exercise control over their information through notice and choice will remain, even as user interfaces shrink or disappear. I frequently urge companies to get creative when it comes to informing consumers about what kinds of information they're

---

[24] 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/.

[25] 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.

[26] *See* IOT REPORT, *supra* note 4, at 13-14.

[27] *See id.* at vii.

[28] *See id.* at 27-33.

[29] *See id.* at 34.

[30] *See id.* at 33.

[31] *See id.* at 37-38.

collecting, and allowing consumers to choose what information to share, and when.[32] Interactive apps and command centers that allow consumers to control the many connected devices in their homes could be very helpful in this regard.[33]

So notice and choice, data minimization, security, and other Fair Information Practice Principles apply to the emerging Internet of Things just as they did to the Internet of PCs, laptops, and smartphones, even though we will have to get more creative about how to apply these principles.

Consumer Privacy Bill of Rights

This leads to a question that has been vigorously discussed here in Washington, in Silicon Valley, and elsewhere: Should rights and obligations based on the Fair Information Practice Principles be incorporated into a baseline privacy law here in the U.S.? My answer is "yes." An appropriate baseline privacy law would accomplish two useful goals: it would provide strong, specific, and enforceable protections for consumers; and it would provide clear rules of the road for businesses.

The Obama Administration deserves credit for releasing a discussion draft that wrestles with some of the difficult issues that go along with baseline privacy legislation. But I am concerned that the discussion draft falls short of providing clear protections for consumers and clear guidance for businesses. The manner in which companies give notice, the kinds of choices that they provide to consumers, and the scope of access to consumers' data would all be subject to how companies interpret the "context" in which they deal with consumers and the level of "privacy risk" that they believe a given data processing activity involves. In my view, the discussion draft relies too heavily on "codes of conduct" and privacy review boards, and contains too few clear, bottom line consumer protections. As we move forward with this legislation, I look forward to working with Members of Congress, the Administration, and stakeholders to craft a bill that puts the "consumer" back in the Consumer Privacy Bill of Rights.

Maintaining Interoperability: The U.S. Privacy Framework and Global Data Flows

Of course, other countries and regions are wrestling with similar questions of how best to protect consumers' privacy in an age of big data and the Internet of Things. In Europe, the proposed EU data protection regulation currently under discussion is designed to update Europe's data protection framework, putting in place a single, modernized privacy law to govern the entire European Union.

This differs significantly from the U.S. privacy regime. Our framework is different from that in the EU and other regions. In the U.S., we have deep protections in certain sectors, including healthcare, education, financial services, credit reporting, and children, and, at the state

[32] *See* Julie Brill, Commissioner, It's Getting Real: Privacy, Security, and Fairness by Design in the Internet of Things, Address at Carnegie Mellon University, at 8 (Jan. 28, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/621381/150128dataprivacyday.pdf.

[33] *Id.*

level, data breach notification. Section 5 of the FTC Act, and the state laws that are modeled on it, apply much more broadly, and will continue to allow us to take action against unfair and deceptive acts and practices involving data collection and use.

I believe it would be beneficial to consumers and businesses around the globe for policymakers to ensure that cross-border data flows take place legally, efficiently, and in a manner that protects consumers, despite the differences in our privacy regimes. For the past 15 years, the U.S.-EU Safe Harbor Framework has been the main tool for allowing companies to transfer personal data from the EU to the United States.[34] However, 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. In the wake of these revelations, the European Commission issued a report on the Safe Harbor commending the FTC's enforcement, indicating overall that the Safe Harbor Framework should be retained, but demanding thirteen changes.[35]

Over the past year, the Department of Commerce and the European Commission have been negotiating eleven of the thirteen changes demanded by the European Commission. Many of the items on the European Commission's list make good sense, and would improve Safe Harbor from a consumer protection standpoint. Two of the European Commission's recommendations for improving Safe Harbor concern national security issues, and are still under discussion.

I am optimistic that the U.S. and the European Commission will work out these remaining differences. The FTC's 24 Safe Harbor enforcement actions[36] and our recent case against TRUSTe based, in part, on its alleged misrepresentations about its Safe Harbor certifications, show that we are serious about enforcing companies' Safe Harbor commitments.[37] And the improvements that Commerce has already put in place should make Safe Harbor a stronger and more effective consumer protections tool – which is precisely what it was designed to be.

* * * * * *

I believe we are all working towards the same goal: protecting consumers and promoting innovation in an increasingly connected, and data driven world. Each of us – companies, consumer groups, advocates, academics, policy makers throughout the world – have important

---

[34] *See* Dept. of Commerce, U.S.-EU Safe Harbor Overview (last updated Dec. 18, 2013), *available at* http://export.gov/safeharbor/eu/eg_main_018476.asp.

[35] *See generally* 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.

[36] *See* FTC, Privacy & Security Update (Jan. 2015), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2014 (stating that the FTC has brought 24 Safe Harbor enforcement cases and listing recent cases).

[37] *See* 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; TRUSTe, FTC Matter No. 1323219 (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/141117trusteagree.pdf.

roles to play in bringing making this vision a reality. I stand ready to work with all of you, and I am optimistic that when we are back together again next year, we will look back and see that we have made real progress together.

Thank you.