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.

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 rop

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

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]

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

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.