UNITED STATES OF AMERICA

Federal Trade Commission

"Our American Privacy"

Remarks of Commissioner Noah Joshua Phillips*

U.S. Chamber of Commerce and the American Chamber of Commerce to the European Union

Brussels, Belgium
October 23, 2018

Good afternoon and thank you for having me. It is an honor to join you today.

I have really appreciated my first ICDPPC gathering. These events, where data privacy officials can cut through the noise and communicate in person, can be invaluable in fostering mutual understanding. We are all here because we care deeply about consumer protection, data privacy, innovation, and growth; and we are all working to get the complicated balance right.

Today, I would like to talk a bit about how we in the U.S. strike that balance, as well as areas where the international community can continue to work together going forward. But before I start, I want to remind you that I speak today for myself, not for the Federal Trade Commission (FTC) or my fellow Commissioners.

Privacy Debate in the U.S.

Data cross borders and industries, with companies adopting business models and offering products and services often unimaginable just a few years ago. Innovation is good – driving value for consumers and the economic growth that comes with it.

But the proliferation of data and its uses pose challenges too, for consumers and the government. That is why, today, we in the United States are engaged in a national conversation about privacy. Citizens, advocates, private industry, and government, recognizing the importance of the issues we confront, are debating, intensely and thoughtfully. And, as I have learned already this week, the world is watching.

* The views expressed below are my own and do not necessarily reflect those of the Commission or of any other Commissioner.

As a guide to the perplexed, or those not following, I want to highlight just a bit of what is happening in the United States right now.

First, the administration has convened a series of meetings and consultations, with both private entities and government agencies, to shape a new federal approach to privacy. Last month, the part of the Commerce Department charged with leading that process, the N.T.I.A. – the National Telecommunications and Information Administration – issued a request for comments on a proposed approach to modernize data privacy policy in the U.S.[1]

The proposal – which focuses on desired outcomes and goals of privacy practices, rather than specific prescriptions on how to achieve them – re-emphasizes many of the principles familiar to those of you who work in this space: transparency, control, minimization, access, accountability, and the like. I am pleased that the proposals also anticipate the continuation of the FTC's lead role in enforcing consumer privacy laws.

Second, as you are undoubtedly aware, the state of California has passed a privacy law.[2] This law requires, among other things, that consumers have a right to know what information has been collected about them; why and from where; how that information is used and with whom it has been shared; the right to opt-out of information sharing; and a right of deletion. It also includes a private right of action for data breaches, although privacy violations are enforced by the Attorney General's office.

That law, which does not go into effect for a couple years, is not without controversy. Even its supporters would, I think, concede that it was passed very quickly and has technical issues that need to be resolved. But regardless how you feel about the law, it has spurred the debate on privacy.

That leads to a third major development, which are a series of hearings in Congress on potential federal legislation. The hearings have incorporated a broad range of voices, including consumer advocates, industry, and even Austrian DPA Director and Chair of the European Data Protection Board, Commissioner Andrea Jelinek, who testified just a couple weeks ago.[3]

In addition, as the U.S. independent agency with primary enforcement authority over data security and privacy, the FTC is an important part of this national conversation. Privacy is also part of the series of hearings on consumer

---

[1] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018).

[2] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.100 *et seq.* (2018).

[3] *Examining Safeguards for Consumer Data Privacy: Hearing Before the S. Comm. on Commerce, Science, & Transportation,* 115th Cong. (2018); *Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the Consumer Privacy Act: Hearing Before the S. Comm. On Commerce, Science, & Transportation,* 115th Cong. (2018) (statement of Dr. Andrea Jelinek, Chair, European Data Protection Board).

protection and competition that the Chairman has convened, the first of their kind in decades.[4] This process will include at least two hearings on data security and privacy in late 2018 and early 2019, which should be announced soon; and there will be public opportunity to comment and share your views in connection with those hearings. We value and welcome your comments.

On the enforcement side, we continue to bring cases. While we normally keep our investigations secret, we have confirmed publicly those into the data breach at Equifax and the Facebook / Cambridge Analytica debacle. We also recently closed our comment period on a proposal to put Uber under order, following its data breach and privacy failures.[5] You can expect continued privacy enforcement from us.

Finally, leading industry players in technology and telecommunications are promulgating privacy principles, and there is market competition over privacy. They are also working on projects that enhance consumer control over data, like the "Data Transfer Project" recently introduced by major technology companies.[6]

The U.S. Model of Personal Privacy

While the interest is renewed because of the increasing role of consumer data in the U.S. economy, and all the activity I have described that flows from it, our national conversation about privacy is nothing new at all.

In 1789, the Drafters of the U.S. Constitution enshrined the Fourth Amendment, stating: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[7] This notion of privacy, the individual as against government, was and remains absolutely fundamental. It developed over time, in ways relevant to our conversation today.

Justice Louis Brandeis, one of the progenitors of the FTC, believed that the Fourth Amendment "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. [The Founders] conferred, as against the Government, the right to be let alone."[8] Brandeis wrote this while living during another period of technological revolution, which saw the advent of readily-available photography and telephonic communication, innovations allowing information about people to be recorded and shared. These changes concerned him, leading him to develop and expand this new concept of "privacy."

---

[4] *See* Fed. Trade Comm'n, *Hearings on Competition and Consumer Protection in the 21st Century* (2018), https://www.ftc.gov/policy/hearings-competition-consumer-protection.
[5] *See* FTC Press Release, *Federal Trade Commission Gives Final Approval to Settlement with Uber* (Oct. 31, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber.
[6] *The Data Transfer Project* (2018), https://datatransferproject.dev/.
[7] U.S. CONST. amend. IV.
[8] Olmstead v. United States, 277 U.S. 438 (1928), (Brandeis, J. dissenting), *overruled* by Katz v. United States, 389 U.S. 347 (1967), and Berger v. New York, 388 U.S. 41 (1967).

The U.S. Supreme Court incorporated this concept into its Fourth Amendment jurisprudence, recognizing the "reasonable expectation of privacy," a balancing test that assumes a zone of personal privacy into which the government may not intrude without substantial justification.[9] This legacy informs our modern jurisprudence and the bevy of U.S. laws enshrining privacy rights against the government, from local law enforcement to our national security apparatus.

For just one example among many, in 1986, Congress passed the Electronic Communications Privacy Act, which updated wiretapping prohibitions and data access for the emerging digital age.[10] Just this summer, in the Carpenter case, the Supreme Court applied the "reasonable expectation of privacy" test to rule that the government needs a warrant to retrieve cell-site records, noting that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[11]

This history is long and deeply ingrained, and the right fundamental, which is why Americans sometimes bristle at the accusation that we do not care deeply about balancing privacy and national security, and wonder why other states, who face the same important issues, are not the focus of similar criticism.

As opposed to several years ago, the U.S. national conversation today is more focused on consumer privacy, and the conduct of the private sector. Here, too, it is important to recognize the United States' priors. Congress has long recognized the need for protections over consumer data, both legislating the U.S. risk-based approach to privacy and granting the FTC enforcement authority.

In 1970, Congress passed the Fair Credit Reporting Act, among the very first laws regulating the collection and use of consumer data by private industry.[12] FCRA , which has been amended and updated over time, establishes the rights of consumers over the credit reporting data collected, shared, and used by private enterprises and reflects principles similar to those set out in the Fair Information Practice Principles, which I will discuss shortly – limitations on use, access and correction rights, data quality rules, FTC enforcement, and the like. Importantly, the FCRA also grants the FTC enforcement authority.

In 1973, a U.S. government study group released a series of Fair Information Practice Principles or FIPPs.[13] These FIPPs – which include principles such as transparency, use limitation, access and correction, data quality, and security – are

---

[9] Katz v. United States, 398 U.S. 347 (1967) (Harlan, J. concurring).
[10] Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
[11] Carpenter v. U.S. 138 S. Ct. 2206, 2217 (2018).
[12] 15 U.S.C. § 1681 *et seq.*
[13] U.S. Dep't of Health, Education and Welfare ("HEW"), *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens,* xx (1973).

recognized as "the building blocks of modern information privacy law,"[14] and are reflected in many or most subsequent data privacy laws and principles. The following year, Congress passed the Privacy Act, which applies to government data collections and which is based on the FIPPs.[15]

Over the last quarter century, Congress has identified specific industries or areas that require additional privacy protections – such as the online activity of children,[16] financial data,[17] and health data[18] – and passed tailored laws to handle those concerns, laws that include enforcement regimes and, where deemed appropriate, civil monetary penalties. And where Congress has not legislated specifically, privacy protections remain, in the form of the FTC's unfairness and deception authority.[19]

Ours is standards-based, outcome-oriented, flexible approach, focused on consumer harm and capable of protecting consumers from harmful practices even as technologies develop and evolve in unanticipated ways. Connected toys,[20] Blockchain,[21] and algorithms[22] are just a few examples of how we apply that broad and flexible authority to new developments in technology and markets. We at the FTC have brought dozens of privacy and data security cases to protect consumers and we will continue to do so.

This dual approach to privacy – risk-based regulation with strong enforcement mechanisms and flexible standards to address deception and unfairness – has allowed the U.S. to balance consumer protection with innovation and competition. We have also avoided risks, like the elimination of competition and the entrenchment of incumbents. The FTC also enforces anti-trust law, which compels us to recognize competition considerations.

---

[14] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999).
[15] Privacy Act of 1974, 5 U.S.C. § 552a.
[16] Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. § 6501 *et seq.* and 16 C.F.R. § 312.
[17] Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. 6801 *et seq.*; Financial Privacy Rule, 16 C.F.R. § 313; Standards for Safeguarding Customer Information, 16 C.F.R. § 314.
[18] Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C. and 29 U.S.C.).
[19] 15 U.S.C. § 45(a)(1).
[20] *See* FTC Press Release, *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act* (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.
[21] *See* FTC Press Release, *FTC Shuts Down Promoters of Deceptive Cryptocurrency Schemes* (Mar. 16, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-shuts-down-promoters-deceptive-cryptocurrency-schemes.
[22] *See* FTC Press Release, *Texas Company Will Pay $3 Million to Settle FTC Charges That it Failed to Meet Accuracy Requirements for its Tenant Screening Reports* (Oct. 16, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed.

That is not to say that we in the U.S. are perfect – as I said earlier, we are engaging in a conversation that may result in modifications – but as a framework, this has served us well, allowing for technological development while continuing to protect consumers.

International Cooperation

Europe and the U.S. differ in how we have approached privacy regulation, reflecting different philosophies and legal traditions, which lead to different privacy regimes and different tradeoffs.

Does this mean that all is hopeless when it comes to European – American privacy relations?

No. I am quite hopeful myself.

We are divided on details, which are often important, to be sure. But not on the motivation – we all want to protect privacy and consumers, making sure that reasonable expectations are met, consumers are not deceived, choices are real and informed, and harmful practices are rooted out, all while fostering trade and innovation.

With that in mind, we can operationalize that good faith by focusing on shared, larger goals. And while I am focusing on Europe and the U.S., these are not exclusive to that relationship.

The first shared goal is, broadly speaking, the interoperability of privacy regimes among those with shared privacy values. We are already working on this with Privacy Shield and as we move forward, we should keep interoperability as a goal that benefits businesses, consumers, markets, and growth.

Where, however, we encounter opposing visions of privacy – governments that would surveil their citizens without limitation, in contrast to the E.U. and the U.S. – we should approach them with appropriate skepticism. Put another way, let us spend less time being critical of friends, and more time evaluating those for whom such criticism is warranted.

Second, and relatedly, we have a shared interest in growth and innovation. Consumers, wherever they are, want similar things from the digital experience: convenience; speed; connection; tools for a better, easier, richer life. We have seen the outstanding growth of such tools over the last twenty years, and our policies and agreements should ensure that we are not inhibiting further development and growth in digital markets.

Finally, we should work closely against real, substantial threats that the digital age poses to our democracies and our economies, to our shared way of life and to a culture of innovation. Our current environment, while possessing enormous potential to enhance culture, democracy, education, and information, also possesses

the seeds that some want to exploit to undermine just that potential through theft, deception, discord, and misinformation. As friends who share values and a vision for how technology can aid society, we should join together against those who seek to undermine those values and that vision.

To this end, we should look for opportunities for information sharing, and joint enforcement collaboration and cooperation, and avoid disputes that could undermine such cooperation. Let us pledge to do our best to understand one another and dedicate ourselves to advancing these shared goals, moving forward as partners.