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 gather2s3 (t)-9f8 (p)4 (p)4 8ID 3 >pr 9( )10.1 (C/4 (t)

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 cott06 Tw 0.2s– obi5htni1-2 ((i)-54)-9 (tI)-4 i-6.9 (ak)8 (p-54)-.(i)-

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 [illegible]0558/9d04 (y)-3 (/465.003 Tw8Y(c)/4 (C)1(t)-12 Tw 0 -ed)4 (.)-2 (T.-4 ( )]TJ 02 (i) ( )]n)0.5 (g

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 –

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,

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 s ociety, 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 go als, moving forward as partners.