United States of America
Federal Trade Commission

A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation

Christine S. Wilson*
Commissioner, U.S. Federal Trade Commission

Remarks at the
Future of Privacy Forum

Washington, DC

February 6, 2020

* The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner. Many thanks to my Attorney Advisor, Nina Frant, for assisting in the preparation of these remarks.

I. Introduction

Good evening. I would like to thank Fernando Laguarda for the kind introduction. I would also like to thank the Future of Privacy Forum for sponsoring this event and supporting important research in the privacy arena. I enjoyed reading the papers that will be honored this evening, and I congratulate the authors on their insightful contributions to the growing body of privacy literature. Before going further, I must add that the thoughts I will share tonight are my own and do not necessarily reflect those of the Federal Trade Commission or any other Commissioner.

We focus tonight on an important and timely topic. Since joining the Commission in September 2018, I have witnessed a growing awareness from consumer groups, business leaders, and policy makers about the importance of consumer privacy. Stakeholders have responded to data breaches, privacy missteps by notable platforms, and the new uses of data like facial recognition and biometric screening with a heightened focus on consumer privacy. Businesses are overhauling their privacy features, companies are marketing the privacy practices of their consumer goods, consumer groups and the media continuously cover stories about the privacy practices and data use of large corporations, and consumers are using ballot initiatives to deman(e)6 manu.3 T(ti

circulated[2]

I'd like to begin my talk by discussing how the information asymmetries that characterize the privacy arena make federal privacy legislation imperative. Then, I will outline other imperatives that support my call for a comprehensive privacy law. Finally, I will discuss some of the privacy principles I hope will be incorporated into any forthcoming privacy legislation.

II. Information Asymmetries Put Consumers at a Disadvantage

Companies have relatively complete information about the characteristics of the goods and services they offer. In a competitive market, competition drives sellers to provide truthful and useful information about their products to consumers.[6] Moreover, competition drives companies to fulfill promises to consumers about price, quality, and other material terms.[7] Dissatisfied buyers can vote with their feet and wallets and go elsew ly ty6 (ed)-4 (b72 (he)-6 (r5 (s)-69oC 8.0

Privacy Attitudes of Smart Speaker Users shows that many consumers do not understand how their data are collected, maintained, and used by smart speaker products.[9] And many consumers lack a basic understanding of the privacy settings available for these products. More than half of the 116 survey participants did not know that (1) companies permanently stored their recordings or (2) they could review their recordings.[10] Interestingly, many of the survey participants who knew they could *review* their recordings did not know they could *delete* them.[11] The study also found that many survey participants did not want their interactions with the smart speaker *permanently* stored[12] and did not want their children's interactions with the device stored *at all*.[13] Malkin and his coauthors highlight the information asymmetry between the privacy expectations of the smart speaker users and the privacy practices of the smart speaker producers.

This paper also helps explain the privacy paradox – that is, the inconsistency between consumers' expressed preferences and their actual behavior when it comes to privacy.[14] Some commentators assert that while consumers *say* they value privacy, they readily give it away – so consumers must not be concerned about privacy practices.[15] In fact, a growing body of research, including papers honored tonight, indicates that information asymmetry and privacy resignation explain the

i

and constrained interoperability that undercut the ability of U.S. companies to compete globally. Federal privacy legislation could help avoid this unnecessary burden on businesses while simultaneously providing appropriate protections for consumers.

Privacy legislation also could address the emerging gaps in sector-specific approaches to privacy laws created by evolving technologies. For example, the Health Insurance Portability and Accountability Act ("HIPAA") applies to certain doctors' offices, hospitals, and insurance companies, but not generally to cash practices, wearables, apps, or websites like WebMD.[27] But sensitive medical information is no longer mostly housed in practitioner's offices. Your phone and watch now collect information about your blood sugar, your exercise habits, your fertility, and your heart health. Because data is ubiquitous, we need a comprehensive federal privacy law.

On the international front, GDPR came into effect in May 2018.[28] Some countries are now adopting various GDPR provisions.[29] Others are striking out on their ow (oupa)4 (ni)-2 c.6P <</MC.5vk[c(

data flows. Global data flows have

courts to respond "flexibly and rapidly to the insistent challenges of new technology on privacy."[35]

That would be welcome news, given that police are accessing an ever-growing universe of commercially significant data during the course of their investigations. Courts have yet to clarify whether consumers can overcome the longstanding third-party doctrine to protect Google Maps information, browser searches, or genealogy information in the hands of corporate entities. What is known, though, is that the pace of technological evolution creates serious privacy risks not addressed by existing Fourth Amendment legal principles.[36] Courts will continue to explore the limiting principles of the Fourth Amendment as applied to commercial repositories of data. In the interim, a comprehensive federal privacy law could establish clear rules, define American values, and entrench protections of our citizens' privacy rights. In the words of Hartzog and Richards, now is the time – the constitutional moment – to make the difficult decisions about the legal, technical, and social structures governing the processing of human information.[37]

IV. Privacy Frameworks

expectations of privacy and the trades they are willing to make with their data. Consequently, the value judgments around privacy are best left to elected officials entrusted by the American public to make those calls.

But many of us would agree that we have identified principles to guide our approach to privacy legislation. Perhaps most notably, **privacy legislation should incorporate the United States' traditional harm-focused, risk-based approach to privacy protections**. In its privacy enforcement cases, the FTC has alleged several categories of injuries including physical injury, financial injury, reputational injury, and unwanted intrusion.[39]

Ignacio Cofone's *Antidiscriminatory Privacy* paper makes the case for addressing another type of harm through legislation – discrimination. Cofone asserts that "decision-makers will be unable to discriminate if they lack the sensitive information to do so,"[40] and that "discrimination is better avoided than compensated."[41]

I agree that legislation should be drafted to address identified harms – but I also agree with Hartzog and Richards that cognizable harms may not be inflicted only on individuals and that we are only beginning to understand and assess the externalities of the data industrial complex.[42] Martin Abrams, the Executive Director of the Information Accountability

---

(1890). Other scholars have argued that privacy turns on the extent to which (1) we are known to others, (2) others have physical access to us, and (3) we are the subject of others' attention. Ruth Gavison, *Privt Td ( )Tj -0.001f 0l/TT2 1 Tf9 Tc 0 Tw*

play in protecting an individual's privacy.[45] Accountability tools, like the Data Protection Impact Assessments (DPIA) required by GDPR or the Algorithmic Impact Assessments suggested by Kaminski and Malgieri, are forms of monitored self-regulation that can engender constructive

engaging in tradeoffs between privacy and competition,[49] and I agree. While there undoubtedly will be some tradeoffs between privacy and competition, I am confident that Congress can design a privacy bill that provides appropriate protections for consumers while maintaining competition and fostering innovation.

In addition to those high-level principles, I would recommend that privacy legislation include a few additional elements:

- First, the FTC should be the enforcing agency. We have decades of experience in bringing privacy and data security cases, and we have the requisite expertise to tackle any new law effectively.[50]
- Second, any legislation should include civil monetary penalties, which Congress has included in other statutes enforced by the FTC, including COPPA[51] and the Telemarking and Consumer Fraud and Abuse Prevention Act.[52]
- Third, the FTC should be given jurisdiction over non-profits and common carriers, which collect significant volumes of sensitive information.[53]
- Fourth, any law should include targeted APA rulemaking authority. That way, the FTC can enact rules both to supplement legislation and to permit adjustments in response to technological developments.[54]

---

[49] Hartzog, *supra* note 1, at 71.
[50] *See* Fed. Trade Comm'n, Media Resources on Privacy and Security Enforcement, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited February 7, 2020) (providing links to privacy and security cases, public events, statements, reports, amicus briefs, and testimony).
[51] Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506 (2018).
[52] 15 U.S.C. §§ 6101-6108 (2018).
[53] For many years, the Commission has testified in favor of eliminating the common carrier exemption. Fed. Trade Comm'n, Prepared Statement of the Federal Trade Commission: "Oversight of the Federal Trade Commission," Before the Subcommittee on Consumer Protection and Commerce, United States house of Representatives Commie Susrers

- Fifth, any law should include preemption. Preemption is key to precluding a patchwork of conflicting state laws