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 demand privacy protections.

We've arrived at a tipping point for privacy, spurred in part by the General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). All eyes are on Congress during this defining moment – or, as authors Hartzog and Richards label it, a "constitutional moment for U.S. privacy identity."[1] And it appears that many in Congress are prepared to rise to the occasion. Notable draft and discussion draft bills recently have been

[1] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1, 8 (forthcoming 2020).

circulated[2] and, appropriately, they identify the FTC as the responsible agency for enforcing new privacy legislation.

The FTC has two missions – competition and consumer protection. Consumer privacy and data security traditionally fall under the umbrella of consumer protection. These two broad missions are related because robust competition is the primary means of achieving optimal outcomes for consumers. In other words, competition gives consumers the protection of competitive outcomes. And perfectly competitive markets maximize the aggregate economic welfare of producers and consumers.[3]

As you can probably tell, I have great faith in markets to produce the best results for consumers. But, as Econ 101 teaches, the prerequisites of healthy competition are sometimes absent. Markets do not operate efficiently, for example, when consumers do not have accurate information about product characteristics.[4] Neither do markets operate efficiently when the costs and benefits of a product are not fully borne by its producer and consumers – in other words, when a product creates what economists call externalities.[5] I believe both of these shortcomings arise in the areas of privacy and data security. In the language of economists, both information asymmetries and the presence of externalities lead to inefficient outcomes with regard to privacy and data security. Consequently, even though I have great faith in markets, I have come to believe that federal privacy and data security legislation is necessary. For purposes of tonight, though, I will focus on privacy.

---

[2] Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 108 (as introduced in the Senate by Senator Cantwell, December 3, 2019), https://www.congress.gov/116/bills/s2968/BILLS-116s2968is.pdf; Senator Wicker, Discussion Draft, United States Consumer Data Privacy Act of 2019, § 201, https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf; *see also* H. Energy & Commerce Comm., Discussion Draft, Bipartisan Data Privacy Bill, 23-25, https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/2019.12.18-Privacy-Bipartsian-Staff-Discussion-Draft.pdf.

[3] ROBERT PINDYCK & DANIEL RUBINFELD, MICROECONOMICS 317 (8th ed. 2017).

[4] *Id*. at 625-26.

[5] *Id*. at 626.

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 elsewhere.

In the absence of perfect information, though, consumers cannot evaluate the quality and value of those offerings. Numerous studies have analyzed information asymmetries with regard to the privacy characteristics of various products and services.[8] And two of the papers honored tonight document the existence of woefully asymmetric information in this arena.

---

[6] Howard Beales, Richard Craswell & Steven C. Salop, *The Efficient Regulation of Consumer Information*, 24 J. L. ECON. 502 (1981) ("[S]ellers have a substantial economic incentive to disseminate information to consumers.").
[7] J. Howard Beales III & Timothy J. Muris, *FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?*, 83 GEO. WASH. L. REV. 2157, 2163-64 (2015).
[8] A 2014 study conducted by Pew Research found that a majority of Americans (incorrectly) believe that when a company posts a privacy policy, it ensures that the company will not share user data. Aaron Smith, *What Internet Users Know about Technology and the Web*, PEW RESEARCH CTR. (Nov. 25, 2014), https://www.pewresearch.org/internet/2014/11/25/web-iq/. Similarly, a 2015 study conducted by researchers at the University of Pennsylvania's Annenberg School of Communication found that 58% of respondents incorrectly believed and 7% responded "don't know" to the prompt: "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission." JOSEPH TUROW ET AL., U. PA. ANNENBERG SCH. FOR COMM., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 16 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf; *see also*, Ginger Zhe Jin & Andrew Stivers, *Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics* 6 (2017), https://ssrn.com/abstract=3006172 (arguing that a consumer is dependent on the representations made by companies or their vendors because he or she is not in a position to review and assess the privacy policies and actual practices of each company in the opaque networks of entities supporting the consumer's digital interactions).

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 so-called privacy paradox.[16] We have discussed the role of information asymmetry:

---

[9] Nathan Malkin et al., *Privacy Attitudes of Smart Speaker Users*, 2019 PROC. PRIVACY ENHANCING TECH. 250, 251 (2019), https://petsymposium.org/2019/files/papers/issue4/popets-2019-0068.pdf.
[10] *Id*. at 260, 263.
[11] *Id*.
[12] *Id.* at 263 (noting the "retention period desired by respondents ranged from one hour to two years, and the median was 28 days").
[13] *Id.* at 264.
[14] *See* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1039-40 (2017); Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* 17 (Nat'l Bureau of Econ. Research, Working Paper No. 23488, 2017); Luvai F. Motiwalla & Xiao-Bai Li, *Unveiling Consumer's Privacy Paradox Behavior in an Economic Exchange*, 23 INT'L J. BUS. INFO. SYS. 307-29 (2016).
[15] *Id*.
[16] Barth, *supra* note 14, at 1046, 1049; *see also* Jorge Padilla, *Privacy and Consumer Coercion: A Review of Economics Literature* 2 (2019) (on file with author).

if users do not understand the privacy characteristics of products and services, they cannot make informed decisions about their quality and value.

The second explanation for the privacy paradox, the concept of privacy resignation, reflects the notion that consumers rationally choose to forego expending significant time and effort protecting personal information.[17] As we all know, it is cumbersome to manage online personal data.[18] For example, Malkin et al. correctly note that manually reviewing and deleting thousands of smart speaker interactions presents an undue burden for users.[19] Moreover, data breaches routinely expose sensitive consumer data.[20] Together, these two concepts of information asymmetry and privacy resignation explain the privacy paradox and defy the notion that consumers do not value their privacy.

Dark Patterns At Scale explores another form of information asymmetry. Websites and apps use misleading wording, take-it-or-leave-it choices, and hidden privacy options (often referred to as "dark patterns") to nudge users toward desired outcomes.[21] The analysis of

---

[17] Hanbyul Choi et al., *The Role Of Privacy Fatigue In Online Privacy Behavior*, 81 COMPUTERS HUM. BEHAV. 42 (2018) (explaining that the "increasing difficulty in managing one's online personal data leads to individuals feeling a loss of control" and that "[f]requent data breaches may make people feel as though they have no control over personal information, and ultimately drive them into a state of resignation about online privacy.").

[18] Hartzog, *supra* note 1, at 53 (noting that mobile apps can ask users for over two hundred permissions and even the average app asks for about five) (citations omitted).

[19] Malkin et al., *supra* note 9, at 262. Hartzog and Richards also note in their paper "even if a company were to somehow deliver perfect information and provide meaningful choices, it wouldn't solve the limited bandwidth we have as human beings limited to one brain…users become burdened, overwhelmed, and resigned to the path of least resistance…so we just click 'agree.'" Hartzog, *supra* note 1, at 53.

[20] Rae Hodge, *2019 Data Breach Hall of Shame: These Were the Biggest Data Breaches of the Year*, CNET (Dec. 27, 2019), https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/. The article does not mention headline-grabbing data breaches at Waze, Wawa, 7-11, T-Mobile, Quest Diagnostic, Flipboard, Dunkin Donuts, and Ascension.

[21] Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM.-COMPUTER INTERACTION 1, 2-27 (2019); *see also* FORBRUKERRADET (Consumer Council of Norway), DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS TO PRIVACY (2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (explaining how "default settings and dark patterns, techniques and features of interface design meant to manipulate users, are used to nudge users towards privacy intrusive options.").

In 2019, Senators Mark Warner and Deb Fischer introduced the DETOUR Act, bipartisan legislation that prohibits dark patterns. Press Release, Senator Mark R. Warner, Senators Introduce Bipartisan Legislation to Ban

thousands of shopping websites revealed that a significant percentage of popular shopping websites deploy design elements that feature hidden costs or subscriptions, false urgency, and hard-to-cancel purchases.[22] I was particularly struck by the use of third-party plugins that facilitate deceptive low-stock messages to create high-pressure sales tactics.[23] These findings may help enforcers identify deceptive online sales tactics and understand other areas where consumers face a lack of transparency.

The bottom line: markets function inefficiently when consumers face significant information asymmetries, including incomplete information about product features and quality.[24] In the face of documented market failures, government intervention may help protect consumers. This is the situation we face in privacy today. Consumers' data is collected, maintained, shared, and monetized in ways that consumers cannot see and cannot avoid. As demonstrated by the FTC's robust enforcement program, some of these practices cause harm. A privacy law can provide needed transparency so that consumers can begin to make informed choices.

III. Other Imperatives

Information asymmetry is one important reason for privacy legislation but there are others, including predictability and guidance for businesses. On the domestic front, businesses need clarity and certainty regarding privacy rules of the road. CCPA became effective on January 1, 2020,[25] and other states are seeking to pass their own privacy laws, creating an emerging patchwork of regulatory frameworks.[26] The result? Burdensome compliance costs

---

Manipulative 'Dark Patterns' (Apr. 9, 2019), https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns.

[22] *See also* Mathur, *supra* note 21, at 13 (listing categories and types of dark patterns).

[23] *Id*. at 20.

[24] PINDYCK, *supra* note 3, at 625-26, 631-56.

[25] Cal. Civ. Code §§ 1798.100-1798.199 (West 2020).

[26] The National Council of State Legislatures found that privacy bills or bill drafts were introduced or filed in at least 25 states and in Puerto Rico in 2019. Nat'l Council of State Legislatures, *2019 Consumer Data Privacy Legislation* (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-

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 own.[30] This growing number of diverging privacy regimes will create incremental hurdles to efficient cross-border

---

privacy.aspx; *see also* Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws: The Modern Data Economy Is Too Big to Regulate at the State Level*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html ("Fourteen states have considered legislation on internet service providers. Twenty-five states and Puerto Rico have considered legislation focused on various aspects of consumer data. All 50 states, the District of Columbia, Guam, Puerto Rico, the Virgin Islands and even some municipalities have their own laws about how to respond to data breaches. All of those laws are subject to change. In 2019, states considered at least 21 measures to amend data breach laws. Over 150 pieces of legislation on consumer data have been considered, and five states passed bills mandating privacy studies to inform future legislation.").

[27] The Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d.

[28] General Data Protection Regulation (EU) 2016/679, 2016 O.J. (L119/1).

[29] For example, Thailand's Personal Data Protection Act takes effect on May 27, 2020. Chusert Supasitthumrong, *The Reach and Liabilities of the Personal Data Protection Act*, BANGKOK POST (Sept. 3, 2019), https://www.bangkokpost.com/business/1741919/the-reach-and-liabilities-of-the-personal-data-protection-act. Brazil's legislature passed the General Data Protection Law, which is scheduled to take effect in 2020. Bruno Bioni et al., Int'l Ass'n of Privacy Prof'ls, *GDPR Matchup: Brazil's General Data Protection Law*, IAPP (Oct. 4, 2018), https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Argentina, too, is considering amendments to its Personal Data Protection Law. Diego Fernandez, Int'l Ass'n of Privacy Prof'ls, *Argentina's New Bill on Personal Data Protection*, IAPP (Oct. 2, 2018), https://iapp.org/news/a/argentinas-new-bill-on-personal-data-protection/.

[30] Personal Data Protection Act 2012 (No. 26 of 2012) (Sing.), https://sso.agc.gov.sg/Act/PDPA2012#P1IV-,; Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c.5 (Can.), https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html

data flows. Global data flows have transformed international trade by establishing digital platforms to export goods, improving efficiency and increasing productivity, reducing barriers to market entry, allowing businesses (including small enterprises) to reach vastly larger markets, and improving global value chains. Consistency among regulatory frameworks reduces company costs, promotes international competitiveness, and increases compliance with privacy standards.[31] Accordingly, a comprehensive U.S. privacy law that enacts a single privacy standard could facilitate global interoperability, helping to bridge the differences between U.S. and foreign privacy regimes.

Permit me to identify one last imperative for federal privacy legislation. Paul Ohm's paper about the Supreme Court's 2018 opinion in *Carpenter v. United States*[32] highlights the risks to our fundamental privacy rights posed by rapidly evolving technology.[33] Yes, the Fourth Amendment protects American citizens from government action, and a federal privacy law will provide guardrails for private actors. But Ohm observes that the "reasonable expectation of privacy" test that has been used in Fourth Amendment cases connects the arenas of government action and commercial data collection. As his paper notes, "the dramatic expansion of technologically-fueled corporate surveillance of our private lives automatically expands police surveillance too, thanks to the way the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine."[34] Ohm's paper argues that the "reasonable expectation of privacy" test should be replaced by the rules outlined in *Carpenter*, allowing

[31] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 9-10 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[32] 138 S. Ct. 2206 (2018).
[33] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J. L. & TECH. 357 (2019).
[34] Ohm, *supra* note 33, at 362.

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 Framework

Having discussed why a freemarketeer like me supports federal privacy legislation, I'd like to highlight the elements I hope to see in a privacy law. Of course, I recognize that the appropriate contours and contents of privacy legislation pose complicated questions. Legal scholars and legislatures have struggled to define privacy.[38] People also differ in their

[35] Ohm, *supra* note 33, at 416.
[36] CYRUS FARIVAR, HABEAS DATA 228-32 (2018).
[37] Hartzog, *supra* note 1, at 79.
[38] Recently, Daniel Solove avoided defining privacy, but instead offered six categories to help conceptualize privacy, which he argues includes the right to be let alone, limited access to the self, secrecy, control of personal information, personhood, and intimacy. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1094 (2002). Scholars have championed each of these concepts over the years. Louis Brandeis and Samuel Warren are often credited with the creation of the modern privacy notion, defining privacy in an 1890 paper as "the right to be let alone." Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 HARV. L. REV. 193, 193

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, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980). In conducting an economic analysis of privacy law, Richard Posner took the position that privacy is secrecy, or the withholding or concealment of information. Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 411, 421 (1978) (arguing that economic theory aligns with the four aspects of privacy covered by common law: preventing the use of one's picture and name without one's consent for advertising purposes, preventing facts about one being portrayed in a "false light," preventing people from obtaining information by intrusive means, and preventing the publication of intimate facts about oneself). Control of personal information, personhood, and intimacy have also found support among privacy experts.

[39] *See* Fed. Trade Comm'n, Comment to the National Telecommunications & Information Administration on Developing the Administration's Approach to Consumer Privacy, No. 180821780-8780-01, 8-9 (Nov. 2018), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

[40] Ignacio Cofone, *Antidiscriminatory Policy*, 72 SMU L. REV. 139, 140 (2019).

[41] *Id*. at 140.

[42] Hartzog, *supra* note 1, at 42-44.

Foundation, has made a similar observation. Specifically, Abrams asserts that an assessment of risks from data use, storage, and processing "should consider the benefits and risks to the individual, for society as a whole, and for the parties conducting big data discovery and application."[43] Using a narrowly circumscribed focus on "data protection" could preclude an appropriate analysis of the societal costs and benefits from data processing, so it will be important to use a holistic approach.

Another area of mainstream consensus involves accountability. **Legislation should require accountability for both privacy and data security practices on the part of entities that handle data**. Simply put, companies should own the risks they create for others. An accountable organization is one that can demonstrate that it has effective internal processes in place to comply with its legal and regulatory obligations. The Centre for Information Policy Leadership (CIPL) has identified elements of organizational accountability: (i) leadership and oversight, (ii) risk assessments, (iii) written policies and procedures, (iv) transparency, (v) training and awareness, (vi) monitoring and verification, and (vii) internal enforcement to address non-compliance.[44]

As noted in the CIPL framework, legislation should also encourage companies to regularly assess and document privacy and data security risks in accordance with written policies and procedures, and to invest in mechanisms to adequately address the identified risks. Kaminski and Malgieri's paper highlights the important role that iterative risk assessments can

---

[43] THE INFO. ACCOUNTABILITY FOUND., UNIFIED ETHICAL FRAME FOR BIG DATA ANALYSIS: IAF BIG DATA ETHICS INITIATIVE, PART A 2 (2015), http://informationaccountability.org/wp-content/uploads/IAF-Unified-Ethical-Frame.pdf. *See also* Information Accountability Foundation Model Legislation U.S., available at http://informationaccountability.org/wp-content/uploads/FairOpenUseAct.9.23.19.FINAL-V2.pdf (Sept. 23, 2019) (noting that, absent accountability, uses of personal data create risk to both individuals and society and that individuals have the right to expect that organizations will process data in a manner that creates benefits for the individual or, if not for the individual, for a broader community of people).

[44] CENTRE FOR INFO. POLICY LEADERSHIP (CIPL), ORGANIZATIONAL ACCOUNTABILITY – PAST, PRESENT AND FUTURE 3 (Oct. 30, 2019), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf.

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 data security and privacy practices. Specifically, these mechanisms require companies to consider the risks of data collection, use, and security, and to develop concrete ways of mitigating those risks.[46] Processes that create a culture of compliance through documentation of compliance choices usher in welcome consumer safeguards.[47]

Another worthy principle: privacy legislation should embrace the notion that **transparency empowers individuals to make informed choices**. As I discussed when highlighting information asymmetries, consumers need clarity regarding how their data is collected, used, and shared. Only when they understand the privacy characteristics of products and services can they effectively evaluate the value of those goods for themselves.

Importantly, the legislative framework should also consider competition. Regulations, by their nature, will impact markets and competition. GDPR may have lessons to teach us in this regard. Research indicates that GDPR may have decreased venture capital investment and entrenched dominant players in the digital advertising market.[48] Hartzog and Richards note that if laws limit certain types of business activities, the pace of innovation may slow and costs may increase. The authors urge legislators to be intentional and transparent when

---

[45] *See* Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations* (Univ. of Colo. Law, Legal Studies Research Paper No. 19-28, 2019), https://ssrn.com/abstract=3456224.

[46] *Id.* at 16.

[47] *See* Christine S. Wilson, Remarks at the Global Antitrust Institute: FTC vs. Facebook, Antonin Scalia Law School 6, 10 (Dec. 11, 2019), https://www.ftc.gov/system/files/documents/public_statements/1557534/commissioner_wilson_remarks_at_global_antitrust_institute_12112019.pdf.

[48] *See* Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment* 4 (Nat'l Bureau of Econ. Research, Working Paper No. 25248, 2018), https://www.nber.org/papers/w25248.pdf; *GDPR - What happened?*, WHOTRACKSME BLOG (2018), https://whotracks.me/blog/gdpr-what-happened.html.

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 Committee on Energy and Commerce 17 (May 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1519212/p180101_house_ec_oversight_testimony_may_8_2019.pdf; Fed. Trade Comm'n, Prepared Statement of the Federal Trade Commission: "Oversight of the FTC," Before the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security of the Committee on Commerce, Science, and Transportation, United States Senate 16 (Nov. 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1423835/p180101_commission_testimony_re_oversight_senate_11272018_0.pdf.
[54] COPPA provides a good example of the appropriate division of labor between Congress and the FTC. There, Congress made the requisite value judgments. For example, Congress determined it was important for websites targeted to children to obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children. 15 U.S.C. §§ 6502. The FTC was then empowered through rulemaking to outline the mechanics of how websites or online services could obtain verifiable parental consent. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5.

- Fifth, any law should include preemption. Preemption is key to precluding a patchwork of conflicting state laws that will unnecessarily burden businesses and hinder domestic and international data flows.

And I'll end the list with something a law should not include – a private right of action, which would allow plaintiffs' lawyers rather than expert agencies like the FTC and state attorneys general to establish a sound and consistent national policy.

V. Conclusion

Thank you again for the opportunity to share with you my thoughts on privacy, data security, and the contents of the excellent papers that we are here to honor this evening. The authors have given us much food for thought, and they have identified useful avenues of further research and potential enforcement. Authors, thank you again for your contributions to this important and growing area of law.