Written Testimony of Julie Brill

Former Commissioner of the U.S. Federal Trade Commission

and

Corporate Vice President,
Chief Privacy Officer,
and
Deputy General Counsel for Global Privacy and Regulatory Affairs

Microsoft Corporation

Before the
Committee on Commerce, Science, & Transportation United States Senate

Revisiting the Need for Federal Data Privacy Legislation

September 23, 2020

I. Introduction

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for again providing me the opportunity to share my views on global privacy law and the need for comprehensive U.S. federal privacy legislation. Much has changed in the world since I was last here in December, and these changes have important implications for privacy law and policy.

My name is Julie Brill. I am Microsoft's Corporate Vice President, Chief Privacy Officer, and Deputy General Counsel for Global Privacy and Regulatory Affairs. I joined Microsoft after nearly three decades of public service dedicated to privacy, consumer protection, and competition, including six years as a Commissioner of the U.S. Federal Trade Commission ("FTC") and more than 20 years working at the state level in roles including Chief of Consumer Protection and Antitrust for the States of North Carolina and Vermont and head of the Privacy Working Group of the National Association of State Attorneys General.

It is in my capacity as a former FTC Commissioner that I am here today, but there is great consistency between what I worked towards at the FTC and what I am now working to achieve at Microsoft. I came to Microsoft because the company shares my long-held perspective that privacy is a fundamental human right, and that privacy is integral to customer trust. Microsoft has provided me a unique opportunity to continue contributing to the future of privacy and consumer protection, because Microsoft is a world leader both in creating the technologies that are transforming people's lives, and in promoting responsible and transparent use of personal information.

Federal Privacy Law is a Critical Need for the United States

Much has changed since I spoke to the Committee last December. We are now experiencing a global pandemic, which is having an enormous impact on the economy, our ability to work, our kids' education, and our ability to remain connected to friends and communities. At the same time, we have experienced a national awakening about the need to address racial inequities.

What has not changed is the urgent need to pass a comprehensive privacy law. In December, I said that a comprehensive privacy law was more urgently needed than ever before. What was merely urgent 10 months ago is absolutely critical now. The degree to which we can come together as a nation to end the coronavirus public health crisis; build a sustainable recovery; and address systemic racism in our society will depend in part on how well and responsibly we use the data that today's digital systems enable us to collect. We would be much better able to responsibly harness data to address the greatest issues of our time if we had a national comprehensive privacy law in place.

The American public deserves better protection of its data. And the American public wants this protection. According to a recent KPMG study, 9 out of 10 American consumers view privacy as a human right.[1]

There have been significant developments in privacy law and policy since December, including implementation of a broad privacy law in California, and the placement of an initiative on the California ballot to further improve the California law. However, the U.S. remains one of the few developed countries not to have comprehensive privacy protections for its people. If this

[1] KPMG LLP, The new imperative for corporate data responsibility (2020), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf.

situation is not rectified soon, the United States will suffer as American businesses will be less able to effectively compete on the global economy.

Testimony Overview

Today, I will discuss with you the significant developments that have occurred in privacy law since the December hearing, the importance of passing a robust privacy law to effectively address the public health crisis and racial inequity, and why passing a privacy law can help American competitiveness and enable companies to responsibly unlock the value of data for the benefit of society.

II. Advancements in U.S. Privacy Law and Policy Since Last Hearing

There has been more activity around U.S. privacy law and policy in the past year than we have experienced at any time in the past three decades. In just the past nine months, we have seen the following significant activity:

- Several strong privacy bills have been introduced this Congress, including by members of this Committee. In particular, the comprehensive privacy bills introduced by Chairman Wicker, Ranking Member Cantwell, Senator Moran, and others are historic in their scope, strength, and sophistication. [2] If adopted, these proposals would be the most robust privacy laws in the U.S., and they would reflect American leadership in the development of global standards for privacy protection.

[2] *he* "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or the "SAFE DATA Act;" S. 2968, the "Consumer Online Privacy Rights Act" or "COPRA;" and S. 3456, the "Consumer Data Privacy and Security Act of 2020."

- The California Consumer Privacy Act ("CCPA")[3] has gone into effect, and the California Privacy Rights Act ("CPRA")[4] qualified for the November ballot.
    - CCPA is the first U.S. privacy law to provide individuals with the means to meaningfully control their data. Microsoft was the first major company to commit to apply the core rights contained in CCPA throughout the United States.
    - More is needed to ensure that the responsibility for protecting privacy is borne by companies, and not just by individuals, which is why the proponents behind CCPA introduced CPRA. If adopted, CPRA would require companies to engage in data minimization and purpose limitation, and to assess the risk of their data collection and use practices. Additionally, CPRA would introduce protections for sensitive data and children, and provide individuals with the ability to opt-out of advertising activities of large companies on third-party websites.
- Washington state has also advanced a bill, the Washington Privacy Act ("WPA"), that would build upon the current global standard for privacy protection.[5] The bill has passed Washington's state senate two years in a row. Earlier this year, a revised version of the bill also passed the House, and a bicameral conference committee nearly agreed on a final version.[6] An updated version of the bill, which adds COVID-related provisions focused on collection and use of health data by both companies and government agencies, was introduced earlier this month.[7]

---

[3] Cal. Civ. Code § 1798.100 *et seq*.
[4] California Attorney General, "Initiative 19-0021A1," The California Privacy Rights Act of 2020 ("CPRA"), https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf, appearing on the ballot as Proposition 24, https://www.sos.ca.gov/elections/ballot-measures/qualified-ballot-measures.
[5] The Washington Privacy Act (Washington SB. 6281).
[6] The Washington Privacy Act (Washington S.B. 6281-S2 AMH ENGR H. 5242.E).
[7] Washington Privacy Act 2021 (DRAFT) (August 5, 2020), http://sdc.wastateleg.org/carlyle/wp-content/uploads/sites/30/2020/09/WPA-2021-DRAFT-Carlyle.pdf.

Each of these initiatives would create a good national model for the United States to provide important privacy protections for people in the United States, and would provide companies with a framework for demonstrating their trustworthiness through the responsible collection and use of data. In addition, each of these initiatives would be interoperable with the European Union's General Data Protection Regulation ("GDPR") and thus allow American companies to compete more effectively on the global stage, [8] and yet they represent uniquely American ideas about how to ensure trust by setting a strong solid standard.

III. GDPR's Influence on Global Norms

GDPR went into effect in May 2018. Since then, many countries have adopted new or modified privacy laws influenced by GDPR, including Brazil, Japan, Kenya, Korea, New Zealand, South Africa, and Thailand.[9] Development of an American privacy law that is nonetheless interoperable with the GDPR and other global privacy laws will facilitate the competitiveness of U.S. companies by enabling them to participate as a trusted provider in these markets, and to avoid the need to architect multiple data systems in order to participate in the global economy.

In addition, the European Court of Justice – in its recent *Schrems II* judgment striking down the EU-U.S. Privacy Shield Framework[10] — has indicated that European privacy norms

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[9] *See* Brazil Internet Law, Law. No. 13,709 of August 14, 2018; Japan Amended Act on the Protection of Personal Information; Kenya Data Protection Act, 2019; Korea Amended Personal Information Protection Act; New Zealand Privacy Act 2020 (effective December 1, 2020); South Africa Protection of Personal Information Act; Thailand Personal Data Protection Act.
[10] Judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, C-311/18, EU:C:2020:559, in part striking down the Privacy Shield Framework, 81 Fed. Reg. 51,042 (Aug. 2, 2016) and Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, 2016 O.J. (L 207).

related to privacy must be ensured by U.S. companies that seek to transfer data about Europeans to the United States. While there are several issues raised in the *Schrems II* decision that will need to be resolved between the U.S. Government and the European Commission in order to clarify the ability of U.S. companies to participate effectively in the European market, the adoption of a federal privacy law will be among the important steps that Congress should take to demonstrate that the United States has a durable national privacy framework.

IV. Components of a Robust Privacy Framework

Microsoft believes that comprehensive federal privacy legislation should support four key principles: consumer empowerment, transparency, corporate responsibility, and strong enforcement.

- **Consumer Empowerment.** Empower consumers with the tools they need to control their personal information, including the ability to make informed choices about the data they provide to companies, to understand what data companies know about them, to obtain a copy of their data, to make sure the data is accurate and up to date, and to delete their data.

  Americans care deeply about having meaningful control over their data. In just the past nine months, from January 1, 2020 to September 18, 2020, Microsoft received over 14 and a half million unique global visitors to its privacy dashboard, where they were able to exercise their ability to control their data. This continued engagement with the control tools we provide included **over 4 and a half million visitors from the United States**, representing the greatest level engagement from any single country.

- **Transparency.** Require companies to be transparent about their data collection and use practices, by providing people with concise and understandable information about what personal information is collected from them, and how that information is used and shared.
- **Corporate Responsibility.** Place direct requirements on companies to ensure that they collect and use consumers' data in ways that are responsible, and demonstrate that they are worthy stewards of that data.
- **Strong Enforcement.** Provide for strong enforcement through regulators, and ensure they have sufficient resources to enforce the legal requirements that organizations must uphold, but also to be well-grounded in the data collection and analysis technologies that are used in the modern digital economy.

These are the key elements that are required to build a robust and lasting U.S. privacy law.

V. Importance of a Privacy Law to Addressing the COVID-19 Crisis

The U.S. unfortunately has not been sufficiently agile in using data to help society address the COVID-19 crisis. One reason for this is we do not have a common understanding of what companies and other organizations can and cannot do with data to address the crisis. For instance, in the absence of comprehensive protections, it has been difficult for U.S. organizations to understand how they can responsibly deploy health-related data that is not covered by the Health Insurance Portability and Accountability Act ("HIPAA"). This has created confusion and friction, and has hindered our ability to create effective technologies that people can trust.

Microsoft recognizes that using data while preserving privacy is critical to addressing the COVID crisis. In the absence of federal privacy legislation to serve as a guide, Microsoft set out

privacy principles that should govern development of digital technologies to address COVID. [11] We are using these principles in our own, numerous initiatives to provide technical solutions, including participating in technical systems that will help individuals understand if they have been exposed to COVID-19,[12] and assisting public health authorities manage their contact tracing caseloads.[13] We have offered these principles for consideration by governments, public health authorities, academics, employers and industries to consider as they develop approaches for addressing COVID-19.

These are our privacy principles for digital exposure notification technologies:

1. Obtain meaningful consent by being transparent about the reason for collecting data, what data is collected and how long it is kept.
2. Collect data only for public health purposes.
3. Collect the minimal amount of data.
4. Provide choices to individuals about where their data is stored.
5. Provide appropriate safeguards to secure the data.
6. Do not share data or health status without consent, and minimize the data shared.
7. Delete data as soon as it is no longer needed for the emergency.

Microsoft takes to heart its responsibility to offer policy and technical solutions to problems like addressing the COVID crisis. However, our principles are not a substitute for a robust privacy law. We need clear national rules that cover the broad swath of personal

[11] Julie Brill and Peter Lee, Preserving privacy while addressing COVID-19 (April 20, 2020), https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/.
[12] Association of Public Health Laboratories (APHL), Bringing COVID-19 exposure notification to the public health community (July 17,2020), https://www.aphlblog.org/bringing-covid-19-exposure-notification-to-the-public-health-community/.
[13] The At Risk Identification And Alert System (ARIAS) is a CRM solution available through Microsoft Dynamics, https://dynamics.microsoft.com/en-us/crm/what-is-crm/.

information to help all organizations understand how they can responsibly use data – including sensitive health data – to develop innovative and trusted technologies designed to address COVID-19.

VI. Importance of a Privacy Law to Promoting Racial Equity

The urgency in adopting a federal privacy law has been further highlighted by the need to address racial inequities that have been laid bare by the COVID crisis. Over the past six months, we have witnessed COVID-19's disproportionate impact on Black Americans, members of other communities of color, and the elderly and other vulnerable populations. These are the communities that most desperately need more tools to help them mitigate the crisis and bring their communities back together. Yet many people in these communities have heightened concerns that personal information collected to address the public health crisis also could be used to harm them. Privacy laws must include measures to protect civil rights – and to ensure that health and other personal information collected to address the COVID-19 crisis is used only to address the crisis and help vulnerable populations.

Microsoft applauds the efforts of the Chairman and Ranking Member of this Committee, as demonstrated in their privacy bills, to recognize the need to include significant protections for civil rights in the context of a privacy law. Including provisions that prohibit inappropriate *and* discriminatory data collection, use and sharing practices will further people's trust that digital technologies will be used to benefit and not harm them. This will be especially important for encouraging greater adoption of responsible digital technologies to help address the very inequities facing certain populations, including the disproportionate impact of COVID-19.

VII. Americans Want and Deserve Strong Privacy Protection

People in the US want and deserve to have their data protected. As I've noted, a recent KPMG study indicates that 9 out of 10 American consumers view privacy as a human right. Further, the KPMG study indicates that while the majority of consumers agree that they have a responsibility to protect their own data (86%), even more say government has an important role to play (90%) and that companies should put data privacy guidelines and policies in place (92%), take corporate data responsibility seriously (91%) and lead in establishing corporate data responsibility (91%).[14] A recent Pew Research Center study resulted in similar findings: a majority of Americans – regardless of political affiliation – strongly favor increased government regulation of companies' use of their personal information.[15]

VIII. Conclusion

Passing a comprehensive federal privacy law is a critical national priority, and the public wants action now. Americans deserve to be protected. Companies want to understand how they can unlock the value of data to address the most pressing issues of our time. And an effective privacy law is needed to ensure American competitiveness and leadership in digital innovation.

Thank you.

---

[14] KPMG LLP, The new imperative for corporate data responsibility (2020), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf.

[15] Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.