Written Testimony of Julie Brill

Corporate Vice President, Deputy General Counsel, and Chief Privacy Officer

Microsoft Corporation

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

Examining Legislative Proposals to Protect Consumer Data Privacy

December 4, 2019

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to share Microsoft's views on the need for comprehensive federal privacy legislation.

My name is Julie Brill. I am Microsoft's Corporate Vice President, Deputy General Counsel, and Chief Privacy Officer. I joined Microsoft after a long career in public service dedicated to consumer protection, competition and privacy, 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.

Microsoft has provided me a unique opportunity to continue contributing to the future of privacy and consumer protection, because it is both a world leader in creating the technologies that are transforming people's lives and in the responsible and transparent use of personal information. During my time at the company, I have met with regulators and customers around the world, and it is clear from these meetings that the time for strong privacy legislation is now.

America Deserves a Comprehensive Privacy Law

We live in a time of remarkable technology-driven change and disruption. How people work, play, shop, and learn about the world has been transformed over the last decade. Industries have been reinvented. New ways to diagnose and treat diseases have emerged. And the way people connect with one another has been reimagined.

Groundbreaking technologies have driven these changes. Cloud computing — which enables governments, companies, and individuals to analyze and derive insights from data at a scale previously not possible — is now the norm, and it is clear that the progress made thus far is only the beginning. For example, the rapid emergence of artificial intelligence and machine learning technologies holds great promise for the future, as does the rise in quantum computing.

These technologies unquestionably will be transformative and impact our daily lives. Even more so than today, they will raise questions about how we protect the privacy of personal information.

Accompanying these technological changes is a global movement to adopt sweeping legal frameworks to enhance consumer privacy and protect personal information. Europe enacted a landmark data protection law that has been in effect since May 2018: the General Data Protection Regulation ("GDPR").[1] New privacy laws have also recently passed or are currently being developed in Brazil, China, India, Japan, Kenya, and Thailand.[2] Each of these legal regimes include some common principles for data protection. And, together, they are defining global baselines for privacy protection.

[1] 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 95/46/EC (General Data Protection Regulation).

[2] *See* Brazilian Internet Law, Law. No. 13,709 of August 14, 2018; China GB/T 35273-2017 Information Technology – Personal Information Security Specification (effective May 1, 2018); India Personal Data Protection Act, 2018 (draft bill); Japan Amended Act on the Protection of Personal Information (effective May 30, 2017); Kenya Data Protection Act, 2018 (draft bill); Thailand Draft Personal Data Protection Act, B.E. 2562 (effective May 27, 2019).

In the United States, California has enacted the California Consumer Privacy Act of 2018 ("CCPA"), which takes effect this coming January.[3] The CCPA was the first comprehensive privacy law to be passed in the United States. Its provisions reflect emerging international norms, including rights for consumers to access and delete their personal information. Other U.S. states are considering new comprehensive privacy laws as well.[4]

These state-level efforts are important, as they demonstrate the need for comprehensive privacy laws in the United States. U.S. privacy law has generally failed to keep pace with advances in technology and to provide Americans with the protections they want and need in this digital age. Unlike Europeans, or Brazilians, or Chinese nationals, Americans today do not enjoy comprehensive privacy protections that apply across the country. As a result, 81 percent of Americans have reported in a Pew Research Center study released last month that they feel they have little or no control over the data collected about them and believe that the potential risks they face from companies' collection of their data outweigh the benefits.[5] Nearly the same percentage of Americans reported that they were concerned about the way their data is being used by companies.

Today more than ever, there is an urgent need for a comprehensive U.S. privacy law that provides strong protections for all consumers in the United States within a framework

---

[3] Cal. Civ. Code § 1798.100 *et seq*.

[4] *See, e.g.*, Washington SB 5376 (introduced Jan. 18, 2019); Minnesota HF 2917 (introduced May 19, 2019).

[5] 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.

that enables human ingenuity and American innovation to continue to thrive. Americans need a comprehensive privacy law because, all too often, they do not have sufficient information about who has access to their personal information, who is using it, and for what purposes. In many cases, the privacy tools currently available to American consumers to exercise choices with respect to their personal information are too complex and place unreasonable burdens on people to utilize them.

At the same time, in light of Cambridge Analytica, the Equifax data breach, and other recent revelations, Americans are also concerned about whether companies are held to sufficiently high standards regarding the protection of personal information, and whether companies are appropriately held to account when failing to live up to those standards. The Pew Research Center study I cited above found that most Americans believe their personal information is *less* secure today than in the past, and have little or no confidence in companies' public accountability with respect to misuse or compromise of their personal information. Given these findings, it is no surprise that the same study found that a majority of Americans — regardless of political affiliation — strongly favor increased government regulation of companies' use of their personal information.

Microsoft's Longstanding Commitment to Privacy

At Microsoft, we believe that privacy is a fundamental human right and that, with recent advances in technology, the protection of this right has become more important and more urgent than ever before. Privacy is also the foundation of consumer *trust*, which is crucial to realize the promise of advanced data-driven technologies. We know that people will only use technology when they trust that it will keep their personal information safe

and secure, and that companies will collect and use consumers' data in ways that are responsible and demonstrate that they are worthy stewards of that data.

Microsoft has continued to put these principles into practice every day through ongoing investments in tools that give consumers greater control over their personal information and greater visibility into how we handle that information. To date, for example, more than 28 million people globally — including more than 10 million Americans — have used our privacy dashboard to better understand and control their personal information. And we have developed a range of products and services that enable our enterprise customers to comply with their data protection obligations and safeguard their users' information as well.[6]

In addition to our privacy-based innovations, Microsoft has long supported and advocated for strong legal frameworks to protect privacy in the United States and around the world. We have been a proponent of comprehensive federal privacy legislation in the United States since 2005.[7] We were also early supporters of the GDPR, and in May 2018 we announced that we would voluntarily extend the rights that are at the heart of the GDPR to all of our customers worldwide.[8] These rights include the right to know about the data we collect about consumers, to access and correct that data, to delete it, and even to take it to

---

[6] Microsoft Trust Center GDPR Overview, https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview.

[7] Microsoft Corp., *Microsoft Advocates Comprehensive Federal Privacy Legislation* (Nov. 3, 2005), https://news.microsoft.com/2005/11/03/microsoft-advocates-comprehensive-federal-privacy-legislation.

[8] Julie Brill, *Microsoft's commitment to GDPR, privacy and putting customers in control of their own data* (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data.

another service if they choose. And just last month, we announced that we would honor the CCPA's core user control rights for consumers throughout the United States, rather than affording them only to California residents.[9]

Microsoft welcomes strong privacy laws like the CCPA in California, in addition to similarly comprehensive privacy laws being considered in other states. The efforts in California and other states have served as important catalysts toward the strong federal privacy law that our country requires and deserves.

Congress should be inspired to build upon these state-led efforts. In addition to granting American consumers the right to control their personal information and establishing strong mechanisms to enforce compliance, we believe that privacy laws should go further by placing more obligations on companies to become responsible stewards of personal information. These accountability requirements should include enhanced transparency about the purposes for which companies collect and use personal information, an obligation to collect and use only the data reasonably necessary for those purposes, and greater responsibility to analyze and improve internal systems to ensure that companies are using personal information appropriately and in line with reasonable consumer expectations. And companies should have affirmative duties to reasonably secure personal information from unauthorized access and to avoid unlawful discrimination in violation of federal and state laws.

[9] Julie Brill, *Microsoft will honor California's new privacy rights throughout the United States* (Nov. 11, 2019), https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights.

Necessary Components for a Strong Federal Privacy Framework

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

Transparency. Transparency is a centerpiece of virtually all data privacy laws existing today. American consumers should have the right to be informed, in a concise and understandable manner, about what personal information companies collect about them, and how that information is used and shared. Companies should provide this information in a context-appropriate fashion at the most meaningful times during the consumer's experience.

Consumer Empowerment. User control is also a central feature of strong privacy laws. American consumers should be empowered to control their personal information and to express their privacy choices in accordance with rapidly-emerging global norms. In particular, consumers should have rights to access, correct, and delete their personal information, and to move their data to other providers.

In addition, Microsoft believes that federal privacy legislation should specifically regulate practices that consumers do not expect and that have a particularly high impact on consumer privacy, such as the collection and sharing of personal information by data brokers that operate behind the scenes, and are unknown to consumers. To ensure that consumers can meaningfully exercise their privacy rights with respect to data brokers, federal privacy legislation should build on concepts from the data broker laws enacted by

Vermont and California.[10] The federal law should require data brokers to register with the federal regulator, and to provide information about the kinds of data they collect and sell, the location of the consumers whose information is affected, and details about how consumers can exercise their data control rights.

Corporate Responsibility. Companies should act as responsible stewards of consumers' personal information, and should be accountable for their actions. This should include affirmative obligations for companies to minimize the amount of personal information they collect — limiting it to the data that is reasonably necessary for the purposes of collection — and to apply technical and other measures to protect that information. Companies also should be required to analyze and improve their internal systems to ensure that they are using consumer data appropriately and in accordance with reasonable consumer expectations, and to document and make these assessments available to an oversight authority upon request. Ultimately, the higher the risk inherent in the proposed use of data, the greater a company's responsibility should be to protect that data. And, as noted above, companies should have affirmative duties to reasonably secure personal information from unauthorized access, and to guard against unlawful discrimination in violation of federal and state laws.

Strong Enforcement. Congress should empower a strong central regulator, such as the FTC, to issue rules and to appropriately enforce the federal privacy law, and should provide the regulator with sufficient authority, technical capability, and funding to do so. This will help to ensure that the regulatory agency has sufficient capacity and expertise to

[10] Vt. Stat. Ann. tit. 9, §§ 2446–2447; Cal. Civ. Code § 1798.99.80 *et seq*.

engage in robust enforcement across the many diverse companies and industries that will be in scope.

A strong federal law should also empower the State Attorneys General to enforce the provisions of the law.

Conclusion

Microsoft appreciates the desirability of diverse proposals, which will lead to more robust discussion and debate about this critically important issue. We particularly appreciate the bills and discussion drafts that have been released by members of this Committee and others. These proposals represent positive steps in the right direction toward a comprehensive federal privacy law.

Since 2005, Microsoft has partnered with members of this Committee to advocate for robust consumer privacy protections, and we are eager to continue to do so. We very much appreciate the good work of Chairman Wicker, Ranking Member Cantwell, and other members of the Committee, and look forward to that work continuing apace.

We urge the members of this Committee to come to a consensus that will allow all American consumers to enjoy the privacy protections that so many others around the world already have.

We are optimistic that Congress will pass comprehensive federal privacy legislation in the very near future, building on the important milestones contained in the CCPA and other state laws. It is past time for the United States to pass meaningful privacy laws that apply to American consumers regardless of where they live in this country. We call on all relevant stakeholders — lawmakers, consumer advocates, industry, government,

academics, and others — to join us in working to pass meaningful privacy protections here in the United States. This is an issue worth fighting for.