Before the
**DEPARTMENT OF COMMERCE**
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**
Washington, DC 20230

| | | |
|---|---|---|
| In the Matter of<br>Developing the Administration's Approach to Consumer Privacy | )<br>)<br>)<br>) | Docket No. 180821780-8780-01 |

**Response of Microsoft Corporation**
**November 9, 2018**

## INTRODUCTION

Microsoft Corporation (Microsoft) welcomes the opportunity to respond to the Request for Comment (RFC) by the National Telecommunications and Information Administration (NTIA) on "Developing the Administration's Approach to Consumer Privacy."

The U.S. has the opportunity to establish a leadership role in the global dialogue about data protection and the administration's recognition of the importance of privacy is an important step. U.S. leadership on these issues is critical for protecting U.S. consumers, our institutions, and industry competitiveness and innovation in this age of digital transformation, especially in emerging technologies such as artificial intelligence (AI). Because of the global aspects of privacy and the desire for the U.S. to be a leader, Microsoft encourages NTIA, and the U.S. government as a whole, to pursue a strong and comprehensive approach to privacy protection that reflects and builds upon global standards.

Microsoft appreciates NTIA's focusing the national discussion on desired outcomes of organizational practices and the high-level goals for federal action. We recognize that the RFC does not call for the creation of a statutory standard. However, we are hopeful that this process will fuel a robust national debate about the most effective approach for comprehensive U.S. privacy legislation.

Our comments provide Microsoft's perspective on the privacy outcomes and goals for federal action raised in the RFC and outline the core tenets of global data protection law that we believe provide the best foundation for comprehensive U.S. privacy law.

**COMMENTS**

## I. Context – Shifting Paradigm

The primary concept of U.S. privacy law has for more than a century been the right "to be let alone." This conception of privacy law has evolved rapidly in light of recent technology-driven change and disruption. Today, because so much of who we are is expressed digitally and so much of how we interact with each other and the world is captured in digital form, people expect to be able to use digital tools and technologies to share data freely and safely with each other and the world. Further, individuals want to be empowered to control how their personal data is used and to trust that the companies with which they share their personal data are being good stewards of that data.

With this shifting paradigm in mind, NTIA is right to question the idea that formal consent from individuals should be the primary goal of legislative approaches to consumer privacy. Further, NTIA is correct that the mechanism for effectuating this consent, notice and choice, has too often resulted in long, legal, regulator-focused privacy notices and check boxes, which don't help the vast majority of individuals.

Indeed, regulators, advocates, academics, and consumers around the world are increasingly skeptical and believe that the shortcomings associated with consent are enabling companies to do what they want with personal data without sufficiently protecting privacy. The implication is that companies are creating user interfaces that influence individuals' decisions and that the sheer volume of processing decisions and lack of information about the processing that takes place behind the scenes make it difficult for individuals to effectively protect themselves. It is important to counter this by requiring companies to protect consumers on an ongoing basis through tools that empower individuals to control how their personal data is used and through continuous risk-based analyses designed to ensure that individuals will be protected throughout the online experience. The goal should be to encourage more companies to do what is best for consumers by providing consumers with control over their data in a manner that also enables the responsible use of data for broader societal and public good.

Microsoft agrees with NTIA that any new privacy framework must (1) engender trust, (2) avoid regulatory fragmentation and promote interoperability with global standards, (3) empower individuals to meaningfully control privacy preferences, (4) provide risk-based flexibility of obligations, (5) and encourage the responsible design of products and services.

## II. Privacy Outcomes

We discuss the following privacy outcomes suggested by the RFC in the section below: Transparency, Control, Risk Management, Reasonable Minimization, Security, Access and Correction, and Accountability. Additionally, we suggest the following additional outcomes: Responsibility According to Role, De-Identification, and Responsible Use of Facial Recognition Technology.

We agree with NTIA that the most important desired outcomes of a new U.S. privacy law should be a reasonably informed user (Transparency), empowered to meaningfully express privacy preferences (Control), as well as products and services that are inherently designed with appropriate privacy protections (Risk Management), particularly in business contexts in which relying on user intervention (i.e., consent) may be insufficient to manage privacy risks.

**1. Transparency**

Transparency is a challenge in the age of big data. Designing user experiences so individuals receive the right notices at the right times and in the most effective manner without unnecessarily disrupting their online experience is more of an art than a science. Effectiveness often hinges on the reasonable expectations of each individual. These reasonable expectations can be set through effective notices that enable an understanding of what happens to personal data and why, delivered at a time that allows for meaningful decision-making.

Providing such transparency is key to earning and maintaining trust in the online world. This will be particularly true in the context of AI and machine learning. Design choices are critical for ensuring a proper level of transparency. The key is delivering the most relevant information in a helpful way that doesn't overload individuals with unnecessary information or choices.

Organizations should be held accountable for the design choices that they make. This can be accomplished by obligating companies to conduct and document proactive risk assessments during the design stage (discussed further in the Risk Management outcome below). These risk assessments should demonstrate to relevant authorities a valid and credible decisional process in designing online experiences. In particular, the documented analyses should demonstrate consideration of the context of data processing, the impacted parties to which the disclosure is being made, and the purpose and desired effect of the disclosure.

We recommend that privacy notices be clear, transparent and meaningful, and include the following information:

- the categories of personal data collected.
- the purposes for which the categories of personal data shall be used and disclosed to third parties, if any.
- the rights that consumers may exercise pursuant to the underlying law (discussed more in the section on Control below).
- the categories of personal data shared with third parties, if any.
- the categories of third parties, if any, to whom personal data is shared.
- the use of automated decision-making, including meaningful information about the logic involved and the significance and envisaged consequences of the automated decision-making.

These requirements are consistent with the standard set by GDPR.

## 2. Control (including Access and Correction)

The U.S. framework that governs access to and use of data should be modernized to promote interoperability and consistency with global data protection standards. Microsoft recognizes that user empowerment is an essential aspect of the fundamental right to privacy. That is why we extended the rights that are at the heart of GDPR – including the right to know what data is collected, to correct that data, and to delete it or take it somewhere else – to our customers around the world (see https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/). What has been striking to us is that the desire for these controls so clearly resonates with Americans. On both an absolute and per capita basis, the largest number of people using our tools to exercise these rights come from the U.S., demonstrating a desire by American consumers for greater control over their personal data (see https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans/).

U.S. legislation should grant consumers the data subject rights that are included in Chapter 3 of the GDPR, particularly the rights:

- To know what data is collected about consumers and the purpose for which data is processed, including:
    - The categories of personal data collected.
    - The categories, if any, of third parties with whom personal data has been shared.
    - Where and how data is used and for what purposes.

- To receive an electronic copy of personal data about the requester that is undergoing processing.

- To request rectification of inaccurate personal data.
    - The preference should be to enable rectification through a secure, automated system that enables consumers to correct their personal data directly. However, the rectification obligation should also be able to be met through manual processes where necessary.

- To delete personal data.
    - Companies should be permitted to retain data if there are "overriding legitimate grounds for the processing." This exception should include the ability to retain data for important security purposes.
    - Companies should also be permitted to retain data when necessary for compliance with a legal obligation, such as laws mandating certain retention periods.

These rights should be applied in a manner consistent with GDPR and should only be granted subject to thorough authentication and verification of the consumer's identity.

### 3. Risk Management (including Accountability)

Microsoft appreciates that risk management is the core of the Administration's approach to privacy protection. We agree with NTIA that a desired privacy outcome is the development of a continuous risk assessment process evaluating whether services are inherently designed with appropriate privacy protections.

Companies should be responsible for ensuring that consumers are protected and safeguarded throughout the online experience. Conducting rigorous and documented risk assessments, which can be reviewed upon request by relevant government authorities, is fundamental to ensuring that consumers are protected and safeguarded. Identified risks should be mitigated through documented safeguards, such that the benefits of processing personal data outweigh the residual risks.

Risk assessments should:

- Cover the processing of all personal data.

- Be conducted prior to planned processing of personal data, any time there is a change in processing that materially impacts the privacy risk to individuals, and on at least an annual basis regardless of changes in processing.

- Identify and weigh the benefits that may flow directly or indirectly from the data processing to the entity conducting the processing, the individuals whose data is being processed, other stakeholders, and the public, against the potential risks to the individuals whose data is being processed, as mitigated by safeguards that can be reasonably employed to reduce such risks. The use of de-identified data (as described in the De-Identification outcome section) and the reasonable expectations of individuals should factor into this assessment.

- Incorporate risk-based flexibility to ensure the ability to derive important benefits from reasonably expected uses of data. The type of data to be used, including whether the data is sensitive in nature, and the context in which the data is to be processed, should be key factors in determining risks and appropriate safeguards.

If the risk assessment determines that the potential risks to the individual whose data is to be processed outweigh the benefits associated with processing the data, then processing should only be allowed to proceed with the individual's informed consent, as provided through an experience that meets the GDPR requirements for consent.

### 4. Responsibility According to Role

NTIA suggests that privacy obligations should vary depending on the role of the entity that is processing data. Specifically, NTIA states that "there should be a distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations." We agree. U.S. law should incorporate the standard distinction between data controllers, which determine the purposes and means of processing personal data, and data processors, which only process personal data on behalf of a data controller and pursuant to a data controller's instructions. This distinction is important because laws that force data processors to independently access and review the data that they process on behalf of data controllers would unnecessarily intrude on the privacy of the individuals whose data the data controllers collected and shared, and likely cause data processors to violate contractual commitments to the data controllers.

Data controllers should be primarily responsible for meeting privacy obligations and for providing redress to individuals. So long as a data processor processes data only on behalf of a data controller, the data processor's responsibility should be to limited to following its data controller's written instructions, including as encapsulated in contracts.

When more than one data controller or data processor involved in the same processing is in violation of a legal privacy obligation, liability should be allocated among such parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among such parties.

We encourage the U.S. government to define these concepts and the relevant obligations attributed to them in a manner consistent with GDPR. This will further global interoperability and help to maintain trust in cloud and AI services, which is so critical for driving innovation.

### 5. Reasonable Minimization

The concept of data minimization – that companies should process personal data only as is necessary in relation to the purposes for processing – has long been a core privacy principle. Data minimization is often perceived as counterproductive to modern data processing, and particularly to the design, development and deployment of AI technologies, systems and services. Indeed, if interpreted narrowly, data minimization obligations could negatively impact the effectiveness and constrain innovation of online services and emerging AI-based systems. Further, restricting access to personal data could make it more difficult for AI models to prevent bias and inequitable outcomes, or enable further verification of systems functionality for safe and reliable outcomes.

A reasonable interpretation of data minimization should understand that the processing of large amounts of data for continuous machine learning is necessary for AI to be accurate and effective, which are basic demands of AI services. Therefore, to meet the data minimization principle, organizations should proactively articulate and document why they need to collect

and process data, why other data sources may be necessary, and what they expect to accomplish by processing the data. This should serve to demonstrate that the data minimization obligation is met because data to be collected or used is relevant and not excessive in relation to the purpose for processing.

### 6. De-Identification

To help address privacy concerns while enabling data collection and use (especially in situations where data is of a sensitive nature) U.S. law should provide significant regulatory relief for implementation of de-identification techniques, which are coupled with legal or administrative controls and commitments not to re-identify data. Defining such de-identified data as being outside the scope of personal data covered by the law would incentivize the development and implementation of de-identification technologies that will substantially increase privacy protection while allowing data to be used for beneficial purposes.

One particularly promising technological approach to de-identification is differential privacy. Developed at Microsoft, this is a technological solution that adds noise to a system to mask data that would otherwise be considered identifiable. When paired with differential privacy or other similar privacy-enhancing techniques, encryption can also help advance de-identification. Researchers are working to develop innovative techniques that would enable data scientists to train AI models on encrypted data, without first requiring decryption.

An all-or-nothing approach that mandates permanently irreversible de-identification is a very difficult (some argue impossible) standard to achieve. Taking a more pragmatic approach to these technologies would enable broader development of AI services while effectively protecting people's privacy at the same time.

To be considered "de-identified data" subject to the broad exceptions contemplated in this section, data controllers should have to:

- Prevent data from being linked to a known natural person without additional information that is kept separate; or

- Modify data to a degree that the risk of re-identification is small, subject that data to a public commitment not to attempt to re-identify the data, and apply one or more enforceable controls to prevent re-identification. Enforceable controls to prevent re-identification may include legal, administrative, technical, or contractual controls.

A data controller or data processor that uses de-identified data should exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject, and should take appropriate steps to address any violations of such contractual commitments.

**7. Responsible Use of Facial Recognition Technology**

Societal concerns about the deployment of facial recognition technology must be addressed, and informed regulation is essential to doing so. We recommend creation of a bipartisan or nonpartisan expert commission to assess the best way to regulate the use of facial recognition technology. This commission should provide the U.S. government with recommendations on the types of new laws and regulations needed, as well as stronger practices to ensure proper congressional oversight of facial recognition technology across the executive branch.

Some of the key issues that should be addressed through government regulation include:

- Should users of facial recognition technology be required to check for accuracy and biased outputs in the population space in which they plan to use the technology?

- What types of legal measures can prevent use of facial recognition for racial profiling and other discriminatory practices while still permitting the beneficial uses of the technology?

- Should consequential uses of facial recognition technology, such as in law enforcement and healthcare scenarios, be subject to human oversight and controls?

- Should providers of facial recognition technology be required to provide customers with information that will help them understand the current capabilities and limitations of facial recognition technology, as well as the risks of improper uses?

- What is the right balance between privacy and public safety when it comes to government uses of facial recognition technology? How can we avoid chilling freedoms of speech, association, and assembly, while recognizing legitimate law enforcement needs?

- Should the law require that companies obtain prior consent before collecting individuals' images for facial recognition? If so, in what situations and places should this apply? And what is the appropriate way to ask for and obtain such consent?

**8. Security (including security breach notification)**

Microsoft agrees with NTIA's inclusion of "Security" in its list of desired outcomes. In determining an appropriate level of security, data controllers should consider the state of the art, implementation costs, and the nature, context and purposes of processing. Further, as should be encapsulated in a risk assessment (per the Risk Management outcome), data controllers should consider the risk of processing to the rights and freedoms of individuals, particularly in the event of a data breach. The level of security offered should be appropriate to reasonably mitigate the risks identified.

Moreover, appropriate federally mandated measures for responding to data security breaches, such as breach notification requirements, should be included in any comprehensive privacy framework.

Federal breach notification law should:

- Require notification of security and privacy breaches where there is a likelihood of harm to individuals.
    - Notices should not be required in cases where the breach does not threaten real harm to the individuals involved; a regime that requires notification even for harmless breaches threatens to engender "notification fatigue" and lead individuals to ignore notices.
    - Over-notification could also potentially make it more difficult for the designated federal privacy regulator to focus resources and attention when material breaches occur. GDPR addresses this issue by excluding from notification requirements breaches that are unlikely to result in a risk to the rights and freedoms of individuals.
- Require notice be provided in a "reasonable timeframe, and without undue delay."
    - It takes time to evaluate the nature and scope of a breach and whether a breach is likely to cause harm to consumers. While it is important to notify impacted consumers in a timely manner, it is more important for the notice to present the facts of the breach fully and accurately. Also, a short turnaround will ultimately shift focus to reporting and administrative burdens rather than breach mitigation. The law should avoid a prescriptive timeframe and instead require notification to be made without undue delay. GDPR and many U.S. state laws, for instance, allow for notification to be delayed for justifiable reasons.

## III. High-Level Federal Goals

Microsoft agrees with the high-level goals introduced by NTIA in the RFC. We believe that these goals can be accomplished in the U.S. In this section we discuss our view on the goals to "harmonize the legal landscape," "provide legal clarity while maintaining the flexibility to innovate," "interoperability" (which we discuss primarily in the context of cross-border data transfer), and "FTC enforcement."

### 1. Harmonize the legal landscape

Microsoft supports NTIA's goal of reducing fragmentation nationally and increasing harmonization and interoperability nationally and globally. Regulatory fragmentation would create a barrier to entry and limit the growth potential of small and mid-size companies, including many of our customers. U.S. privacy law should be interoperable with GDPR.

We need a uniform national framework which protects privacy by giving people stronger control of their personal data. Additionally, as our customers need to be protected now, we will work with states as they develop strong privacy legislation that avoids fragmentation with existing legal obligations and promotes consistency.

**2. Legal clarity while maintaining the flexibility to innovate**

We agree with NTIA that an ideal privacy framework would ensure that organizations have clear rules for legal certainty, while enabling flexibility for novel business models and technologies, as well as the ability to use a variety of methods to achieve consumer privacy outcomes. Technology-specific legislative language can get outdated quickly. Laws should be as technology neutral as possible.

**3. Interoperability (Cross-Border Data Transfer)**

Ensuring that U.S. privacy law is interoperable with global privacy and data protection law should be a top priority. Microsoft's intelligent cloud, intelligent edge and AI strategies rely on an internet that is interoperable, open, and globally accessible to as many people as possible.

Data should be able to flow across borders. This can be accomplished under the current accountability approach, whereby the entity that has collected and transferred the data remains accountable for the continued protection of the data at the same level of protection regardless of where it flows. Ensuring this protection when data is transferred to third countries is critical to meeting obligations under the EU-U.S. Privacy Shield and EU Standard Contractual Clauses.

The ability to deliver high-quality cloud services (e.g., availability, reliability, security) relies on the smooth functioning of the internet infrastructure, and the minimization of geographically conflicting regulations (e.g., cross-border data flows, interoperable privacy frameworks). This functionality can best be protected through strict application of the accountability approach.

Even if a comprehensive U.S. privacy law incorporates the accountability approach, however, a growing number of countries are imposing strict cross-border transfers restrictions. Any U.S. approach to privacy must therefore be able to interoperate and work with these restrictions and new cross-border transfer mechanisms that are being developed.

We recommend that the U.S. leverage existing bilateral and multilateral frameworks to enable companies to use established principles and mechanisms to protect the privacy and security of personal data as it moves across borders. The EU-U.S. Privacy Shield, for example, offers a bilateral cross-border data transfer framework that works well. The APEC Cross-Border Privacy Rules (CBPR) system is another promising multilateral approach. We are encouraged that the CBPR program was validated by the new United States-Mexico-Canada Agreement (USMCA) and is expanding.

We strongly encourage countries to engage in bilateral and multilateral conversations about making the various cross-border transfer frameworks interoperable, such that one standard can be followed for compliance with multiple legal regimes.

### 4. FTC enforcement

It will be beneficial for the U.S. to develop a data protection framework that is applied consistently to different industries. This can be best accomplished by generally allocating data protection oversight to the Federal Trade Commission (FTC), rather than unnecessarily dividing regulatory oversight. Strong FTC enforcement capability, coupled with state attorney general enforcement, will be necessary to effectuate meaningful requirements.

## IV. Global Leadership

An appropriate legal framework for data protection provides an essential foundation for data-driven innovation and entrepreneurship to flourish. It will also strengthen the U.S. position to take a leadership role in relevant dialogues around the world to protect U.S. competitive interest, especially as governments around the world develop policy and regulatory frameworks that restrict data access and flow. With such frameworks in place, the U.S. can also more proactively engage in shaping policy developments, including the upcoming OECD review of its Privacy Principles and similar discussions in other international forums.

## V. Next Steps

Microsoft would like to see U.S. privacy legislation that meets or exceeds current global standards. We are hopeful that the items that NTIA raises in the RFC, in consideration of comments by Microsoft and other responders, will drive legislative efforts and ultimately be considered in legislation.

We recommend that NTIA continue working with interested public and private sector stakeholders toward a goal of formulating a meaningful federal privacy framework. The outcomes and goals identified in the RFC are the right ones. We would like to see them applied in the U.S. and proliferate around the world. This would improve interoperability and reduce the number of inconsistent requirements.

Nothing the U.S. government does on privacy will be meaningful globally until the U.S. has a comprehensive privacy law that provides protections that are at least on par with global standards. It is time for the U.S. to take meaningful action to maximize both privacy protection and innovation and to maintain its competitive advantage.

## VI. Conclusion

The U.S. has an opportunity to be a global privacy leader. We appreciate NTIA issuing its RFC and taking an important step towards that goal. We look forward to partnering with NTIA and to providing further input as this process continues.