BILLING CODE: 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 180821780-8780-01]

RIN 0660-XC043

Developing the Administration's Approach to Consumer Privacy

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice; request for public comments.

SUMMARY: On behalf of the U.S. Department of Commerce, the National Telecommunications and Information Administration (NTIA) is requesting comments on ways to advance consumer privacy while protecting prosperity and innovation. NTIA is seeking public comments on a proposed approach to this task that lays out a set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy, and a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections.

DATES: Comments must be received by 11:59 p.m. Eastern Daylight Time on **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Written comments identified by Docket No. 180821780-8780-01 may be submitted by email to privacyrfc2018@ntia.doc.gov. Comments submitted by email should be machine-readable and should not be copy-protected. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department

of Commerce, 1401 Constitution Avenue, NW, Room 4725, Attn: Privacy RFC, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Travis Hall, Telecommunications Policy Analyst, Office of Policy Analysis and Development, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230; telephone: 202-482-3522; e-mail: thall@ntia.doc.gov. For media inquiries: Anne Veigle, Director, Office of Public Affairs, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4897, Washington, DC 20230; telephone: (202) 482–7002; email: press@ntia.doc.gov.

SUPPLEMENTARY INFORMATION:

I. Background

The U.S. Department of Commerce (Department) requests comment on ways to advance consumer privacy while protecting prosperity and innovation. Every day, individuals interact with an array of products and services, many of which have become integral to their daily lives. Often, especially in the digital environment, these products and services depend on the collection, retention, and use of personal data about their users. Users must therefore trust that organizations will respect their interests, understand what is happening with their personal data, and decide whether they are comfortable with this exchange. Trust is at the core of the United States' privacy policy formation. Through this Request for Comment (RFC), the Administration will determine the best path toward protecting individual's privacy while fostering innovation. The time is ripe for this Administration to provide the leadership needed to ensure that the United States remains at the forefront of enabling innovation with strong privacy protections. A

growing number of foreign countries, and some U.S. states, have articulated distinct visions for how to address privacy concerns, leading to a nationally and globally fragmented regulatory landscape. Such fragmentation naturally disincentivizes innovation by increasing the regulatory costs for products that require scale. The Administration hopes to articulate a renewed vision, one that reduces fragmentation nationally and increases harmonization and interoperability nationally and globally.

Further, changes in the way personal information is used by organizations, and how users interact with the products and services with which they frequently engage, have increased the belief that users are losing control over their personal information. As seen in data collected by the National Telecommunications and Information Administration (NTIA), at least a third of online households have been deterred from certain forms of online activity, such as financial transactions, due to privacy and security concerns.[1] The Adminstration takes these concerns seriously and believes that users should be able to benefit from dynamic uses of their information, while still expecting organizations will appropriately minimize risks to users' privacy. Risk-based flexibility is therefore at the heart of the approach the Administration is requesting comment on in this RFC. We are mindful of the potential impact of a solution on small and mid-sized businesses, and we will be looking for solutions that support their continued ability to innovate and support economic growth.

The United States has a history of providing strong protections for privacy dating back to 1789, with the drafting of our Bill of Rights, including the Fourth Amendment. The United

[1] NTIA Blog, "Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds" (Aug. 20, 2018), https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

States also has been a leader in developing privacy norms, be it through the development of what ultimately became known as the Fair Information Practice Principles (FIPPs) in the 1970's, or through the strongest privacy enforcement regime in the world. For users of products and services in several sectors (e.g., healthcare, education, financial services), specific laws cover how organizations handle personal information. Where no sector-specific laws apply, the Federal Trade Commission (FTC) has the authority to ensure that organizations are not deceiving consumers or operating unfairly. In all respects, the United States has successfully investigated and taken enforcement actions against organizations that violate these existing Federal laws. This RFC asks how best to strengthen the protections users currently enjoy; it does not propose changing current sectoral federal laws.[2]

This RFC is the outcome of an interagency process led by the National Economic Council (NEC) of the United States. NTIA has worked in coordination with the International Trade Administration (ITA) to ensure consistency with international policy objectives, and in parallel with the work of the National Institute of Standards and Technology (NIST) in developing a voluntary risk-based Privacy Framework as an enterprise risk management tool for organizations. In developing this RFC, the Department conducted significant outreach to a diverse set of individuals and organizations, including a broad range of industries, academics, and civil society organizations. These meetings helped to shape this Administration's proposed general approach to privacy, described below.

This approach is divided into two parts: (1) a set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy

[2] These sectoral laws include, but are not limited to, the Children's Online Privacy and Protection Act, Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Fair Credit Reporting Act.

policy, and (2) a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections. This Administration is approaching this subject with humility, an understanding of the complexity of the issues at hand, and a commitment to a transparent process. As such, this RFC does not call for the creation of a statutory standard. Rather, it is looking to commenters to respond with details as to how these privacy outcomes and goals can be achieved. These comments will help to inform future Administration policy, actions, and engagement on consumer privacy.[3]

A. Privacy Outcomes

Principle-based approaches to privacy, particularly when written to be operationalized, often encapsulate the desired outcome and the means used to achieve this outcome. For example, the consent of an informed user is the end-goal of most approaches to consumer privacy, but in order to create legal clarity, this principle is implemented by mandating notice and choice. To date, such mandates have resulted primarily in long, legal, regulator-focused privacy policies and check boxes, which only help a very small number of users who choose to read these policies and make binary choices.

The Administration is instead proposing that discussion of consumer privacy in the United States refocus on the outcomes of organizational practices, rather than on dictating what those practices should be. The desired outcome is a reasonably informed user, empowered to meaningfully express privacy preferences, as well as products and services that are inherently designed with appropriate privacy protections, particularly in business contexts in which relying on user intervention may be insufficient to manage privacy risks. Using a risk-based approach,

[3] This Request for Comment is focused solely on private collection, use, storage, and sharing of personal data. It does not address lawful government access to such data.

the collection, use, storage, and sharing of personal data should be reasonable and appropriate to the contex. Similarly, user transparency, control, and access should be reasonable and appropriate relative to context This outcome underpins many of the principle-based approaches, including the FIPPs. The Administration is proposing that these outcomes be operationalized through a risk-management approach, one that affords organizations flexibility and innovation in how to achieve these outcomes.

Protecting both privacy and innovation requires balancing flexibility with the need for legal clarity and strong consumer protections. Being overly prescriptive can result in compliance checklists that stymie innovative privacy solutions. In addition, a prescriptive approach does not necessarily provide measurable privacy benefits. An outcome-based approach emphasizes flexibility, consumer protection, and legal clarity can be achieved through mechanisms that focus on managing risk and minimizing harm to individuals arising from the collection, storage, use, and sharing of their information.

The following outcomes are provided to spur comments, discussion, and engagement on how best to achieve user-centric privacy outcomes in a manner that is both flexible and clear, not to propose the text of a legal standard. They should be read as a set of inputs for building better privacy protections into products and services. For example, Access and Correction (item 5, below) is not an abstract requirement. Rather, organizations should consider the overall context in which the product or service operates, including the purpose of the product or service, the privacy risks that the product or service may be creating, other means of mitigating these privacy risks, the impact of access and correction on other organizational risks, and other relevant factors, in order to determine the degree or manner in which access and correction could help achieve a user-centric privacy outcome without creating needless costs.

1. **Transparency.** Users should be able to easily understand how an organization collects, stores, uses, and shares their personal information. Transparency can be enabled through various means. Organizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users. In many cases, lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding. Organizations should use approaches that move beyond this paradigm when appropriate.
2. **Control.** Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations. However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information. The controls available to users should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making. In addition, controls used to withdraw the consent of, or to limit activity previously permitted by, a consumer should be as readily accessible and usable as the controls used to permit the activity.
3. **Reasonable Minimization.** Data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm. Other means of reducing the risk of privacy harm (e.g., additional security safeguards or privacy enhancing techniques) can help to reduce the need for such minimization.

4. **Security.** Organizations that collect, store, use, or share personal information should employ security safeguards to secure these data. Users should be able to expect that their data are protected from loss and unauthorized access, destruction, use, modification, and disclosure. Further, organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data; they should meet or ideally exceed current consensus best practices, where available. Organizations should secure personal data at all stages, including collection, computation, storage, and transfer of raw and processed data.
5. **Access and Correction.** Users should have qualified access personal data that they have provided, and to rectify, complete, amend, or delete this data. This access and ability to correct should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization's legal obligations, or the ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation.
6. **Risk Management.** Users should expect organizations to take steps to manage and/or mitigate the risk of harmful uses or exposure of personal data. Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes.
7. **Accountability.** Organizations should be accountable externally and within their own processes for the use of personal information collected, maintained, and used in their systems. As described below in the **High-Level Goals for Federal Action** section, external accountability should be structured to incentivize risk and outcome-based

approaches within organizations that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes. Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data.

B. High-Level Goals for Federal Action

The Administration is also looking to gather feedback on the following high-level goals for Federal action. These goals should be understood as setting the broad outline for the direction that Federal action should take, in addition to comments on the goals, we are also looking for comments with details as to how these goals can be achieved. Below is a non-exhaustive and non-prioritized list of the Administration's priorities. We understand that there is considerable work to be done to achieve these goals.

1. **Harmonize the regulatory landscape.** While the sectoral system provides strong, focused protections and should be maintained, there is a need to avoid duplicative and contradictory privacy-related obligations placed on organizations. We are actively witnessing the production of a patchwork of competing and contradictory baseline laws. This emerging patchwork harms the American economy and fails to improve privacy outcomes for individuals, who may be unaware of what their privacy protections are, and who may not have equal protections, depending on where the user lives. Steps need to be taken to ensure that the regulatory landscape for organizations that process personal data in the United States remains flexible, strong, predictable, and harmonized.
2. **Legal clarity while maintaining the flexibility to innovate.** The ideal end-state would ensure that organizations have clear rules that provide for legal clarity, while enabling flexibility that allows for novel business models and technologies, as well as the means to

use a variety of methods to achieve consumer-privacy outcomes. The Administration understands that balancing legal clarity, flexibility, and consumer privacy requires compromise and creative thinking. It is in striking this balance, however, that the United States has been able to maintain international leadership in both innovation and privacy enforcement, and any future action should strive to create a system that to the greatest extent possible maximizes each.

3. **Comprehensive application.** Any action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data in activities that are not covered by sectoral laws. The differences between business models and technologies used should be addressed through the application of a risk and outcome-based approach, which would allow for similar data practices in similar context to be treated the same rather than through a fragmented regulatory approach.
4. **Employ a risk and outcome-based approach.** Instead of creating a compliance model that creates cumbersome red tape—without necessarily achieving measurable privacy protections—the approach to privacy regulations should be based on risk modeling and focused on creating user-centric outcomes. Risk-based approaches allow organizations the flexibility to balance business needs, consumer expectations, legal obligations, and potential privacy harms, among other inputs, when making decisions about how to adopt various privacy practices. Outcome-based approaches also enable innovation in the methods used to achieve privacy goals. Risk and outcome-based approaches have been successfully used in cybersecurity, and can be enforced in a way that balances the needs of organizations to be agile in developing new products, services, and business models

with the need to provide privacy protections to their customers, while also ensuring clarity in legal compliance.

5. **Interoperability.** The growth and advancement of the Internet-enabled economy depends on personal information moving seamlessly across borders. However, the Administration recognizes that governments approach consumer privacy differently, creating the need for mechanisms to bridge differences, while ensuring personal data remains protected. The Administration should therefore seek to reduce the friction placed on data flows by developing a regulatory landscape that is consistent with the international norms and frameworks in which the United States participates, such as the APEC Cross-Border Privacy Rules System.
6. **Incentivize privacy research.** The U.S. Government should encourage more research into, and development of, products and services that improve privacy protections. These technologies and solutions will include measures built into system architectures or product design to mitigate privacy risks, as well as usability features at the user-interface level. These innovations require more research into understanding user preferences, concerns, and difficulties, as well as an understanding of the impact on legal obligations of third parties and the ability of third parties to exercise other rights provided by law. Privacy research will inform the development of standards frameworks, models, methodologies, tools, and products that enhance privacy.
7. **FTC enforcement:** Given its history of effectiveness, the FTC is the appropriate federal agency to enforce consumer privacy with certain exceptions made for sectoral laws outside the FTC's jurisdiction, such as HIPAA. It is important to take steps to ensure that the FTC has the necessary resources, clear statutory authority, and direction to enforce

consumer privacy laws in a manner that balances the need for strong consumer protections, legal clarity for organizations, and the flexibility to innovate.

8. **Scalability:** The Administration should ensure that the proverbial sticks used to incentivize strong consumer privacy outcomes are deployed in proportion to the scale and scope of the information an organization is handling. In general, small businesses that collect little personal information and do not maintain sensitive information about their customers should not be the primary targets of privacy-enforcement activity, so long as they make good-faith efforts to utilize privacy protections. Similarly, 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. Just as organizations should employ outcome-based approaches when developing privacy protections for their customers, the government should do the same with its approach to privacy enforcement and compliance.

II. Request for Comment

A. Through this RFC, the Department is first seeking feedback on what it believes are the core privacy outcomes that consumers can expect from organizations.

1. Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?
2. Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes are described?
3. Are there any risks that accompany the list of outcomes, or the general approach taken in the list of outcomes?

B. The Department is also seeking feedback on the proposed high-level goals for an end-state for U.S. consumer-privacy protections.

   1. Are there other goals that should be included, or outcomes that should be expanded upon?

   2. Are the descriptions clear? Beyond clarity, are there any issues raised by how the issues are described?

   3. Are there any risks that accompany the list of goals, or the general approach taken by the Department?

C. The Department is seeking comments that describe what the next steps and measures the Administration should take to effectuate the previously discussed user-centric privacy outcomes, and to achieve an end-state in line with the high-level goals. In particular:

   1. Are there any aspects of this approach that could be implemented or enhanced through Executive action, for example, through procurement? Are there any non-regulatory actions that could be undertaken? If so, what actions should the Executive branch take?

   2. Should the Department convene people and organizations to further explore additional commercial data privacy-related issues? If so, what is the recommended focus and desired outcomes?

   3. What aspects of the Department's proposed approach to consumer privacy, if any, are best achieved via other means? Are there any recommended statutory changes?

D. The Department understands that some of the most important work in establishing privacy protections lies within the definitions of key terms, and seeks comments on the defintions. In particular:

1. Do any terms used in this document require more precise definitions?
2. Are there suggestions on how to better define these terms?
3. Are there other terms that would benefit from more precise definitions?
4. What should those definitions be?

E. One of the high-level end-state goals is for the FTC to continue as the Federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction. In order to achieve the goals laid out in this RFC, would changes need to be made with regard to the FTC's resources, processes, and/or statutory authority?

F. If all or some of the outcomes or high-level goals described in this RFC were replicated by other countries, do you believe it would be easier for U.S. companies to provide goods and services in those countries?

G. Are there other ways to achieve U.S. leadership that are not included in this RFC, or any outcomes or high-level goals in this document that would be detrimental to achieving the goal of achieving U.S. leadership?

Instructions for Commenters

This is a general solicitation of comments from the public. We invite comments on the full range of questions presented by this RFC and on issues that are not specifically raised. Commenters are encouraged to address any or all of the questions above. Comments that contain references to specific court cases, studies, and/or research should include copies of the referenced materials along with the submitted comments. Commenters should include the name of the person or organization filing the comment, as well as a page number on each page of the submissions. All comments received are a part of the public record and will generally be posted on the NTIA website, www.ntia.doc.gov/privacyrfc2018, without change. All personal identifying

information (for example, name or address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

Dated: September 21, 2018.

David J. Redl,

Assistant Secretary for Communications and Information, National Telecommunications and Information Administration.

[FR Doc. 2018-20941 Filed: 9/25/2018 8:45 am; Publication Date: 9/26/2018]