Travis Hall, Telecommunications Policy Analyst
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230
Attn: Privacy RFC
(via email at privacyrfc2018@ntia.doc.gov)

November 9, 2018

Re: Developing the Administration's Approach to Consumer Privacy (Docket No. 180821780-8780-01)

Mr. Hall,

Thank you for the opportunity to comment on the National Telecommunications & Information Administration's (NTIA) proposal on data privacy.[1] We welcome the leadership demonstrated by NTIA in this proposal. However, there is still room for improvement. Below we provide general comments on the structure and framing that we believe will better serve NTIA's goals and intent. We then respond to specific questions posed by NTIA.

About Access Now:

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.[2] By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission we operate a global helpline for users at risk to mitigate specific threats. Additionally, we work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those most at risk.

General Observations

A. Privacy is about more than consumers

The thrust of the NTIA's proposal specifies the need "to advance consumer privacy." However, in the internet age privacy protections must extend far beyond consumers. Many of the tools and services used by people today are not goods in the traditional sense - people do not pay

[1] https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy; *See also* https://www.federalregister.gov/documents/2018/10/11/2018-22041/developing-the-administrations-approach-to-consumer-privacy (extending deadline for comment).
[2] https://www.accessnow.org/.

to use them and they do not receive a tangible product. However, this does not mean that there are not significant privacy implications.

For example, users' social media services are probably not "consumers" within the traditional definition, but these services should undoubtedly be subject to any data privacy rules or regulations. Further, while a person may choose to share a piece of information, taken in aggregate millions of data points creates privacy implications at the societal level. Even more troubling online is the passive collection of information from entities like data brokers with whom people may never interact with at all. In fact, these companies may maintain and sell comprehensive data profiles on people who have never heard their name or know they exist. For these reasons, focusing solely on "consumers" is both short sighted and potential harmful to this process. We recommend that the Administration instead focus on the risks to and rights of all people in the United States.

B. Trustworthiness - not trust - should drive data privacy in the United States

NTIA's proposal states, "[u]sers 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." Counter-intuitively, this framing puts the obligation to act to ensure data privacy on people instead of on the companies themselves. However, rather than people needing to blindly offer trust to companies, it is the companies that must demonstrate that they are worth of receiving and processing user data. It is also the responsibility of companies to provide people with sufficient information in a manner that facilitates their understanding of the scope and purpose of that processing.

As the proposal notes, many Americans have refrained from engaging in important online activities, including economic and civic activities.[3] Since this study, the scope and scale of privacy and security incidents have only increased, affecting billions of users of some of the largest companies in the world, from Facebook to Equifax. No amount of trust would have mitigated the harm caused by these incidents, and preventing future breaches requires affirmative efforts from and changes in behaviour from companies.

These are more than pedantic observations. Several of the NTIA's goals are only served if people are served by a data privacy framework, not obligated to it. At the moment, companies are the only entities in a position to take steps to understand the full scope of their data processing, including the third parties who they transmit data to and the various ways they use that data to make decisions about people. A framework that goes beyond checkboxes and compliance mechanisms must respect this reality to drive companies to act in a way that respects and responds to the needs of the people whose data they are using.

---

3 https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

C. A user-centric approach requires that risk is centered on the user

The self-identified "heart" of the NTIA proposal is "risk-based flexibility." While we emphasize the importance of affirmative rights and obligations, we believe it is important for entities that process data to understand and mitigate risk whenever possible.[4] However, there are many entities to which risk can be assessed - risk to the data processor, risk to the general public, or risk to the individual person, to name only a few.

Last year, the U.S. National Institute for Standards and Technologies (NIST) published, "an Introduction to Privacy Engineering and Risk Management in Federal Systems."[5] A central and vital tenet of that report was the observation that, "[a]n effective privacy risk model must capture the potential cost of problems to individuals."[6] In order to ensure that the proposal stays "user centric," NTIA should follow this model and ensure that the risk management element of the proposal refers specifically and clearly to the risk of the person to whom the data pertains.

Focusing on the person seems like common sense, but the norm has been to focus exclusively on the entity collecting data, not the person whose data was being collected. This meant considering the users only by proxy, in the form of legal or reputational costs. That approach has been wholly inadequate for taking into account the wide range of threats created by data processing, and the harm that may be caused by failure to protect that data (such as the emotional impact of having our personal photos revealed to the world).

D. State-level legislation must be allowed to help drive innovation

Broad federal preemption of data privacy laws will stunt innovation and undermine the protection of data. The NTIA proposal claims "fragmentation naturally disincentivizes innovation by increasing the regulatory costs for products that require scale." While this may be superficially true, it fails to consider how privacy itself is a driver of innovation, and state laws are drivers of privacy, as we have recently seen with the recently passed California law facilitating national conversations.

States are more nimble than the federal government - either the executive or legislative branches. State legislators can respond more efficiently and effectively to rapid developments in technology. By keeping preemption out of the proposal, or strictly limiting its scope, NTIA will leave room for states to identify, analyze, and where necessary, respond to emerging gaps in privacy law in the future, which may once again prompt federal action.

At the same time it is not assured, as the NTIA proposal implies, that the absence of full federal preemption will lead to meaningful fragmentation. Today, we see several states considering

[4] See https://www.accessnow.org/data-protection-in-the-united-states-heres-what-we-need-to-protect-the-users/.
[5] https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[6] *Id*. *See also* https://www.accessnow.org/new-report-helps-u-s-federal-agencies-protect-privacy-companies-use/.

privacy laws in direct response to the absence of a federal standard. However, a strong national law could remove the pressure of the total absence of protections moving lawmakers to act unless future shifts in technology or business practice require it.

Responses to Request for Comment

A. Privacy Outcomes

NTIA has asked for feedback on the thoroughness and clarity of the privacy outcomes identified in the proposal, as well as any risks that the identified outcomes may pose.

Transparency - To realize transparency as an outcome, the description must expressly extend to transparency into how organizations disclose information to third parties. Any entity that processes data should not only ensure that people easily understand how they process data, but specifically identify any entity that data may be disclosed to, what data may be disclosed, and the nature of the relationship between the entity and the third party. This information shall be proactively communicated to people, who should also be notified of any updates in these practices.

Control - Along with transparency, meaningful user controls to opt into non-necessary data collection and data disclosure practices can empower people. Control should include considerations of social context, including how people interact, or don't interact, with the relevant entity. Further, the proposal would benefit from a more thorough description of what practices may be considered "reasonable," particularly in regard to entities with no first-person relationship to the person about whom data is processed.

Reasonable Minimization - Noting our recommendation that the risk assessed is risk to the person directly, the level of "acceptable risk" determined by the data processor should be disclosed to the person to whom the data relates in a manner that aids understanding of their exposure. Access controls should also be considered as mechanisms to reduce risk.

Security - All data processed by any entity should be secured.

Access and Correction - It is necessary that the proposal include greater detail about what is meant by "qualified access" to personal data. Further, this right should extend not only to the data a person "provides," but to any data pertaining to that person, with exceptions to protect the exercise of human rights. Further, more work should be done to understand what impact deletion rights will have on AI training sets and how to preserve those rights while preserving the ability to use AI tools in a respectful manner.

Risk Management - Any strategy that prioritizes risk mitigation must recognize that there will always be some risk that cannot be mitigated and provide for cessation of any processing that creates risk in excess of what can be controlled.

Accountability - An effective accountability structure must provide a pathway to a private right of action for people who have suffered harm from direct action of a data processor.

Processing and Purpose Limitations - We urge NTIA to include new outcomes for limitations on the bases and purpose for processing data. Data processing should be limited to specific bases, enumerated by law. These may include for example, meaningful, opt-in consent, execution of a contract, or as otherwise necessary under law. The bases for processing data should be identified by the entity, along with the purpose for which that processing is conducted. Acceptable purposes should be prevented from including any use that is discriminatory or has an overly vague description. These purpose limitations must contemplate the most harmful business models - such as those used by data brokers. Without these limitations, the other outcomes fail to provide necessary levels of protection.

B. Proposed High-Level Goals

NTIA has asked for feedback on the thoroughness and clarity of the proposed high-level goals identified in the proposal, as well as any risks that the identified outcomes may pose.

Harmonize the federal landscape; Legal clarity while maintaining the flexibility to innovate - As discussed above, an approach that prohibits state action on privacy governance may stunt privacy innovation and harm users. Further, the identified goal of a "flexible" approach is best realized by providing space for state action in the future. We recommend NTIA prioritize a strong privacy framework over preemption.

Comprehensive application; Scalability - NTIA is correct that protections must apply to all private sector organizations. A truly comprehensive approach should also apply to government and public interest entities. Further, this proposal must extend to all organizations that process data, including third-party vendors, who must be held to the same standards as any other data processor, with few potential exceptions (such as for employee data for small entities).

Employ a risk and outcome-based approach; FTC enforcement - While a risk-based approach may allow for flexibility, such an approach needs to be accompanied by strong penalty provisions as well as agency guidance in the form of interpretive regulations. Without these elements this approach is rife for misuse and abuse. This can be seen in a historic analysis of the European data protection model. Many of the protections in the General Data Protection Regulation (GDPR) are nearly identical to

those in the Data Protection Directive (DPD) that preceded it in 1995. However, companies frequently bypassed or outright ignored the DPD's requirements due to the weak penalties that it carried for non-compliance, as observed in how many changes entities started to implement when GDPR came into force. We strongly encourage NTIA to make strong penalties and regulations a integral part of their proposal.

Interoperability - The most effective method of ensuring international operability is to learn from the approaches of other entities and ensure that the protections contained in a U.S. approach are at least as strong, if not moreso. This will not only reduce inefficiencies for data processors needing to comply with multiple legal regimes, but help create certainty for data flows between jurisdictions.

Incentivize Privacy Research - In order to actualize the NTIA's stated goal of "more research into, and development of, products and services that improve privacy protections," we highly recommend pursuit of a program that preferences government procurement of products and services from companies that utilize business methods that are not built or supplemented by personal data or data-driven advertising. Grant programs could also be created that fund entities who are investing in privacy-protective business models and practices or approaches that facilitate interoperability. These programs could be funded through penalties levied on entities who fail to comply with the proposed standards. Government entities can also help by demonstrating a commitment to privacy and security themselves, including committing to protecting and facilitating more robust digital security means and methods and exploring best practices for implementing these provisions in certain sectors, such as the internet of things.

C. Next Steps and Measures

Ultimately, a statutory solution is necessary for ensuring meaningful protection for personal data. However, some measures, like the grant program discussed above, can be adopted by the Administration immediately and have an important impact on the data economy. Further discussions may be helpful in determining the full scope of the proposal, but such discussions need to ensure that representatives across various stakeholder groups are on equal footing to the greatest extent practicable, else corporate interests take over the conversation.

D. Definitions

NTIA's proposal would greatly benefit from inclusion of definitions for various terms, including risk, "reasonable," personal information, and sensitive information, though we recommend that any personal information be treated as sensitive information to prevent an unnecessarily narrow approach to protections. We have provided suggestions for some of these terms throughout this document.

E. Federal Trade Commission Authority

If the Federal Trade Commission is intended to act as the primary regulator for privacy protections, it must be given significantly greater resources and authority to carry out its extended mission.

F./G. International Trade; United States Leadership

Discussions on standards of data protection should be kept separate from trade talks and only included in agreement(s) and arrangement devoted exclusively to transfers of personal data, negotiated by experts in that policy area. By nature, trade policies tend to consider legislations protecting users as a barrier to trade. This creates an inherent push for a lowering of standards to the detriment of rights and the interests of people. A lowering of standards would undermine trust in the digital economy as privacy and data protection laws contribute to the free flow of data globally by ensuring a high level of protection for the information shared and contributing to the security of the infrastructure. Accordingly, we urge NTIA to specify that international trade negotiations or debates at the World Trade Organisation are not a forum to discuss measures for the protection of privacy nor an adequate place were to establish new standards.

Conclusion

We appreciate the NTIA's engagement with the privacy community and trust this feedback will assist the agency in refining and improving its current proposal. We look forward to continuing to work with your office to promote strong data privacy standards.

Thank you,

Amie Stepanovich
U.S. Policy Manager
Access Now

Estelle Massé
Global Data Protection Lead
Access Now

Nathan White
Senior Legislative Manager
Access Now