Date: November 9, 2018

Comment from the Internet Society on the
National Telecommunications and Information Administration's
Request for Comments on Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780-8780-01

The Internet Society is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comment, *Developing the Administration's Approach to Consumer Privacy*.

The Internet Society is a global not-for profit organization that supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society. The Internet Society works in partnership with our global community, comprised of over 110,000 members, 136 chapters and special interest groups, and 149 organizational members. It is also the organizational home of the Internet Engineering Task Force (IETF)[1] and the Online Trust Alliance (OTA)[2].

Privacy and the Internet

Privacy is an important right and an essential enabler of autonomy, dignity, and freedom of expression for individuals. The ability for individuals to interact online without sacrificing their personal privacy is key to reinforcing user trust on the Internet[2]. This trust is critical, as it is the foundation of all Internet transactions. When privacy is undermined it diminishes user trust, thereby diminishing the value of the Internet and harming users.

All personal data collectors and handlers should view themselves as custodians of their users' data – protecting their personal data not only as a business necessity, but also on behalf of the individuals themselves.[3] These organizations have a responsibility to uphold end-user privacy and be transparent as to how personal data is being collected and used. By taking a proactive approach to the protection of personal data collected via the Internet, companies can help ensure that their customers have trust in their online communications and transactions.

In the wake of several large-scale data breaches[4] and revelations about the mishandling of data[5], many users and governments have begun to ask what more can be done to protect users from inappropriate collection, use or disclosure of their personal data. Government agencies, such as NTIA, can play an important role in empowering citizens by ensuring their online environment is safe, trusted, and beneficial to all by outlining and encouraging strong data protection rules, such as those outlined in the annex.

---

[1] Internet Engineering Task Force https://www.ietf.org/
[2] https://otalliance.org/2018-online-trust-audit-methodology
[3] https://www.internetsociety.org/globalinternetreport/2016/
[4] https://www.internetsociety.org/blog/2017/10/current-approach-data-handling-isnt-working-equifax-breach-illustrates/
[5] https://www.internetsociety.org/blog/2018/04/larger-facebook-cambridge-analytica-question-really-signed/

A. High Level Principles

The Internet Society applauds NTIA's proposal to focus on actions that will lead to consumers being "…a reasonably informed user, empowered to meaningfully express privacy preferences" as well as products and services being "inherently designed with appropriate privacy protections, particularly in business contexts in which relying on user intervention may be insufficient to manage privacy risks."[6] While the Internet Society supports NTIA's privacy outcomes, they may be further strengthened to better support consumer privacy in the United States. For instance, it is not enough for users to express their privacy preferences: they also need to be honored by companies.

Several of the proposed principles call on organizations to take actions that are largely left up to their wide discretion, which has the potential to limit NTIA's ability to achieve its desired outcomes. For example, the *Risk Management* and *Accountability* principles each call for organizations to "take steps" to mitigate risk, and the *Security* principle only recommends organizations "employ security safeguards" and "take responsible security measures." Each of these principles could be strengthened by calling on organizations to implement current best practices, not just "security measures" or "steps".

Also, while a risk management approach to consumer privacy could be successful, it is crucial that such an approach mitigates risk to consumers (whose personal data may be incidentally collected) and third parties, rather than solely risk faced by data handlers. Too often risk management approaches aim to minimize risk to the data handler, not to the individuals whose personal data they hold. For some data handlers, the risk that poor security or privacy creates may not extend to them. Instead, it may seem riskier to spend resources on data security and privacy than to use them elsewhere in the business.[7]

To strengthen NTIA's privacy principle regarding risk management, we suggest that the sixth privacy principle be revised to read:

"Organizations will apply best practices to manage and/or mitigate the risks that harmful uses or exposure of personal data pose to consumers …"

This similarly applies to data minimization. Data handlers often collect far more personal data than is necessary for their product or service to function, unnecessarily increasing the risk of harm from a data breach or from its inappropriate use. Data handlers should be encouraged to collect only the personal data they need to offer the service and should only keep that data for so long as it is actually necessary. In the case of a data breach, research suggests that the majority of financial and other costs will fall on parties other than the data handler, most often the consumer.[8] Therefore, we suggest that the third privacy principle, *Reasonable Minimization*, emphasize managing risks to the consumer. It could be revised to the following:

---

[6] https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf
[7] https://www.internetsociety.org/blog/2017/10/current-approach-data-handling-isnt-working-equifax-breach-illustrates/
[8] https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf

"… 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 consumer privacy harm. …"

The NTIA should also give consideration to the new ways in which personal data will be collected in the near- and long-term, and how these principles would apply. For example, the ubiquity of Internet of Things (IoT) devices in homes, schools, places of work, and public areas has led to the mass collection of personal consumer information. Unlike online services, where users are often aware that they have interacted with the service (even if they do not know their personal data has been collected), individuals may be unaware that they have interacted with an IoT device at all, let alone given it their personal data. This leads to new questions about the ways in which data is collected, how it is used and how it should be protected.

As "smart city" devices become increasingly common, individuals in public spaces may unknowingly have information collected about them in settings they would not normally expect. They may be unable to understand what personal data has been collected, how they can exercise control over their data, or how to opt-out of its collection. In the case of a breach, it may be impossible to notify all impacted individuals. In certain cases, these devices may be necessary for public safety or other public policy objectives, but it is important to consider how users may be affected and what privacy implications this entails. Additionally, it is important that personal data collected for public purposes in this context is not used for secondary commercial purposes.

Through consultations with privacy and technology experts, NTIA could consider how the privacy rules that hold in the digital world can be applied to the emerging intersection of the digital and physical world.

B. High-Level Goals for Federal Action

NTIA's goals to both "harmonize the regulatory landscape" and "FTC enforcement" are parallel ideals. In the absence of a dedicated privacy enforcement authority in the United States, the Federal Trade Commission (FTC) should continue to be empowered to act as the authority tasked with enforcing federal privacy rules in the United States by ensuring it has adequate resources and capacity.

NTIA also lists "incentivize privacy research" as one of its key goals. While incentives to carry out research are one important aspect, it is important to ensure that those involved represent a broad range of stakeholders. The best way to create strong frameworks is through a multistakeholder process. Multistakeholder decision-making is accountable, sustainable, and leads to wide-spread buy in for policy outcomes. It is inclusive in nature, and the more inclusive it is, the stronger its outputs become.

Multistakeholder processes have led to many successful developments for the Internet. For example, the Internet Society's Online Trust Alliance (OTA) initiative has brought together both public and private sector organizations to develop best practices for consumer privacy, security, and trust. Additionally, OTA assesses the practices of organizations using these best practices and publicizes which organizations are living up to the standards set by the group, and those that

are not.[9] This approach allows organizations to set realistic, yet forward-thinking, goals for themselves and their peers, and yields a set of principles that is able to continuously improve as the technology and marketplace change.

The Internet Society has also led a collaborative process in Canada to develop a shared-responsibility approach and policy recommendations to strengthen IoT security. The Canadian Multistakeholder Process: Enhancing IoT Security[10] has been carried out in partnership with the Canadian government, CIPPIC,[11] CANARIE,[12] and The Canadian Internet Registration Authority (CIRA). The group has convened several in-person and virtual meetings over the past eight months to address consumer education, network resiliency, and labeling for IoT devices. Participants have included representatives from the government, academia, technical sector, public interest groups, and university students. Including all of these voices and encouraging their participation has led to a more robust and well-rounded understanding of the state of IoT security in Canada, and the role each stakeholder group can play in enhancing security. In 2019, the Internet Society will build on the success of this project by engaging in a second, year-long project to enhance IoT privacy.[13]

A similar process in the United States may be valuable to determine what privacy standards are needed for effective consumer privacy, and how all stakeholder groups can work together to uphold those standards. NTIA and other government agencies, including the FTC, could collaborate on this process and evaluate what additional resources are needed to ensure user privacy is protected online.

Conclusion

The Internet Society appreciates the opportunity to share our views with the NTIA on its Request for Comments on Developing the Administration's Approach to Consumer Privacy. By making consumer privacy a priority and engaging with stakeholders, the United States Government will help ensure the Internet is safe, trusted, and beneficial to all.

[9] https://otalliance.org/TrustAudit
[10] https://iotsecurity2018.ca/
[11] Samuelson-Clushko Canadian Internet Policy and Public Interest Clinic https://cippic.ca/
[12] https://www.canarie.ca/about-us/
[13] More details will be released in early 2019.

Annex 1

All Internet companies must take a stand for privacy. They can do so by stepping up their privacy practices and following what Christine Runnegar outlines as a "privacy code of conduct," in a recent op-ed in *The Hill*[14]. Runnegar writes that all data handlers should aspire to achieve the following principles:

1. **Adopt the mantle of data stewardship** - Companies should act as custodians of users' personal data – protecting the data, not only as a business necessity, but also on behalf of the individuals themselves. (In some circumstances, this may mean putting users' interests first and collecting, using and sharing less personal data.)
2. **Be accountable** - Companies should be transparent about their privacy practices, adhere to their privacy policies and demonstrate that they are doing what they say. They should establish clear safeguards for handling personal data and show how those safeguards are being enforced. They should commit to periodic independent audits of their practices and ensure processors or partners are abiding by the same high standards. When something goes wrong, companies should be transparent about what happened, do the best they can to contain the harm, provide affected individuals with meaningful remedies and endeavor to prevent any recurrence.
3. **Stop using user consent to excuse bad practices** - Companies should not rely on user consent to justify the legitimacy of their data handling practices. They should openly demonstrate that their practices are lawful, fair and in the interests of the user before seeking user consent. Users should not be asked to agree to data sharing practices that are unreasonable or unfair, or that they have no hope of understanding.
4. **Provide user-friendly privacy information** - Companies should give users "in time" information about how their personal data is being collected, used and shared. The information should be relevant, straightforward, concise and easy to understand.
5. **Give users as much control of their privacy as possible** - Users should be able to see, simply and clearly, when and how their data is being used. Companies should give users easy-to-use privacy controls and make privacy the default, not an optional extra. User permissions should not be persistent: they should have a limited duration and be specific to the task at hand (e.g. making a video call).
6. **Respect the context in which personal data was shared** - Companies should confine the use of personal data to the context in which it was collected. They should not allow unauthorized or unwarranted secondary uses of personal data.
7. **Protect "anonymized" data as if it were personal data** - Companies should apply basic privacy protections to "anonymized" data to mitigate potential harm if the data is later re-identified or used to single out particular individuals.
8. **Encourage privacy researchers to highlight privacy weaknesses, risks or violations** - Companies should invite independent privacy experts to audit new services and features as they are being developed. As much as possible, the results of those audits should be made publicly available. Companies should also encourage privacy researchers to report privacy vulnerabilities or violations and provide an open transparent process for responsible disclosure.

[14] https://thehill.com/opinion/cybersecurity/401725-why-companies-shouldnt-wait-for-regulation-to-step-up-their-privacy

9. **Set privacy standards above and beyond what the law requires** - Companies should set the next generation of privacy standards. For example, they could consider how to extend privacy protections to the personal data of non-users that has been uploaded by users, and better ways to handle privacy preferences of group data (e.g. a group photo).