Date: August 20, 2018

Comment from the Internet Society on the
Federal Trade Commission's

Competition and Consumer Protection in the 21st Century Hearings
Project Number P181201

Section 4: The intersection between privacy, big data, and competition

The Internet Society (ISOC) is pleased to submit these comments in response to the Federal Trade Commission's (FTC) Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201[1].

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)[2] and the Online Trust Alliance (OTA)[3].

Consolidation

This request for comments comes at an opportune time, as the Internet Society is currently working on its *2018 Global Internet Report*, which will focus heavily on issues of consumer protection and consolidation. The report is due to be published in November 2018 and we hope that it will prove useful as the FTC continues its consultations into 2019.

An important component of the research for this report is a survey of more than 1500 respondents on the topic of "consolidation in the Internet economy". Understood as growing forces of concentration, vertical and horizontal integration, and fewer opportunities for market entry and competition, our consideration of this topic includes the impact of consolidating forces on all stakeholders as well as on the Internet's underlying and evolving technology.

[1] Federal Trade Commission (20 June 2018). *Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201.* [Press release]. Retrieved from: https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st
[2] Internet Engineering Task Force: https://www.ietf.org/
[3] Online Trust Alliance: https://otalliance.org/

We selected this theme because findings from the *2017 Global Internet Report*[4], and developments since its release, indicate increasing concerns about a growing concentration of power in the Internet Economy. They point to market and technical forces that may be driving consolidation at different 'layers' of the Internet, from traffic to communications providers to applications, as well as processes of vertical integration that allows for some companies to own the user experience at every stage and in an increasingly wide range of human activity. As users experience the Internet through a smaller number of providers, for example, there is the potential to restrict our access, choice and future ability to innovate. On the other hand, consolidation is not a new phenomenon, but can be expected as markets and industries mature. To some, it is an evolution foremost characterized by lower prices and better services available to more people.

As many parts of daily life that used to be offline are integrating with the digital world, users are simultaneously experiencing the Internet through an increasingly smaller number of service and content providers. Consolidation and increased digitization could make users more reliant on the choices made by a small group of major players. It may also make them more susceptible to potential future harms, such as restrictions on access, choice, and innovation, should those companies choose advantageous business practices over consumer protection.

It is important that a small number of actors not be allowed to significantly impact Internet users' experience, or to create "too big to fail" scenarios.

The Internet Society encourages the FTC to pay close attention to market trends and to facilitate environments in which robust competition in Internet infrastructure and service markets can flourish. Policies that encourage competition, improve user experience and protect consumers online will play a crucial role in increasing investments in the connectivity market, fostering innovation, improving telecommunications infrastructure, and driving down prices. As the Internet Society found in its report, *Ensuring Sustainable Connectivity in Small Island Developing States*, increased competition will ensure that more users, in more places will be able to access and afford the Internet, and the many resources it offers.[5]

Competition, strong privacy, and consumer protection are also necessary to empower users to take control of their online experience, including demands for increased privacy and security. With increased choice in the market and better protections, there will be stronger incentives for companies to provide products and services with better security and privacy features.

Consumer protection, privacy, and competition for emerging technologies

Competition is particularly important as new technologies develop and are introduced to the market, such as artificial intelligence (AI) and the Internet of Things (IoT). AI and IoT offer huge potential benefits to consumers, but both also pose significant risks in terms of privacy and

[4] Internet Society. (18 September 2017). *2017 Global Internet Report: Paths to Our Digital Future.* Retrieved from: https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[5] Internet Society. (26 May 2017). *Ensuring Sustainable Connectivity in Small Island Developing States.* Retrieved from:https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC_Small_Island_Developing_States-201706015.pdf

security. These technologies enable, and in many cases, rely on the mass collection of user data in order to function. In a consolidated market without incentives to protect consumers, this may have wide-spread, adverse effects for all users.

The full scope of this data collection is often not evident to the data subjects, and consent (when sought and granted) is arguably not fully informed, as consumers often do not know or understand the full scope and risks of the current and potential future use of the data. In some cases, the terms of services and privacy policies are intentionally obscure, and take the form of non-negotiable adhesion contracts.[6]

The FTC is well positioned to help protect US consumers from these risks. To begin, it could encourage or require that fair and easily understandable terms of services and privacy policies be used so that consumers can fully understand the implications of their use of IoT devices and services. As the Internet Society stated in its *2017 Global Internet Report*, policymakers, and regulators like the FTC, should also consider the impact of user data when evaluating any future mergers between Internet content or service providers.[7]

Further, with regard to IoT security, we wish to draw the FTC's attention to the policy recommendations the Internet Society published in its paper *IoT Security for Policymakers*,[8] including:

- **"Ensure legal certainty**: Provide clear, predictable, and enforceable rules requiring IoT providers, developers, and manufacturers to protect against known vulnerabilities by ensuring reporting mechanisms are in place, supporting their products and systems with security patches and updates, and having clearly defined security patch and update policies, including an end date. Especially in the consumer IoT market, security protections should be opt-out, not opt-in.
- **Strengthen consumer protection**: Personal data collected or used by IoT, especially sensor data, should be protected by privacy and data protection laws. Governments can facilitate better security and privacy by clarifying how existing privacy, data protection and consumer protection laws apply to IoT. Similar to the prohibition of misleading representations about product safety, companies should also be prohibited from making misleading or deceptive representations about the security of their IoT products or services. Retailers should also share the responsibility and not sell IoT products with known critical safety and security defects.
- **Clearly assign liability**: To address uncertainty, governments should clearly assign liability on those that are most able to exercise control over the security of a product or service. IoT manufacturers and importers should be liable for safety and security defects in their products."

---

[6] Cornell Law School. *Adhesion Contracts*. Retrieved from: https://www.law.cornell.edu/wex/adhesion_contract_%28contract_of_adhesion%29

[7] Internet Society. (18 September 2017). *2017 Global Internet Report: Paths to Our Digital Future.* Retrieved from: https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[8] Internet Society. (19 April 2018). *IoT Security for Policymakers*. Retrieved from: https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/

The FTC may also wish to consider the principles for AI and consumer protection that the Internet Society has laid out in its *Artificial Intelligence and Machine Learning: Policy Paper*,[9] including the following:

- **Ensuring accountability**: Policymakers should ensure that legal accountability is ensured when human agency is replaced by the decisions of AI systems.
    - Governments should ensure legal certainty on how existing laws and policies apply to algorithmic decision-making and the use of autonomous systems to ensure a predictable legal environment. This includes working with experts from all disciplines to identify potential gaps and run legal scenarios. Similarly, those designing and using AI should be in compliance with existing legal frameworks.
    - Policymakers need to ensure that any laws applicable to AI systems and their use put users' interests at the center. This must include the ability for users to challenge autonomous decisions that adversely affect their interests.
    - Governments working with all stakeholders need to make some difficult decisions now about who will be liable in the event that something goes wrong with an AI system, and how any harm suffered will be remedied.
- **Open governance**: Policymakers, like those at the FTC, should work in a multistakeholder manner to develop processes related to the management and governance of AI. Four key attributes should be upheld in this process: inclusiveness and transparency; collective responsibility; effective decision making and implementation; and collaboration through distributed and interoperable governance.
- **Public empowerment:** AI system designers and builders should be encouraged to be transparent about how their systems are built so that policymakers and the public can understand how the technology works and question its outcomes.

Specific issues regarding big data and privacy

It is critical that consumers are able to make informed choices about collection and use of their data. In a recent op-ed[10], we advocated that organizations should not wait for regulation and adopt a "privacy code of conduct" that includes the following principles:

1. Adopt the mantle of data stewardship
2. Be accountable
3. Stop using user consent to excuse bad practices
4. Provide user-friendly privacy information
5. Give users as much control of their privacy as possible
6. Respect the context in which personal data was shared
7. Protect "anonymized" data as if it were personal data
8. Encourage privacy researchers to highlight privacy weaknesses, risks or violations
9. Set privacy standards above and beyond what the law requires

[9] Internet Society. (18 April 2017) *Artificial Intelligence and Machine Learning: Policy Paper.* Retrieved from: https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper/

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

There are some key privacy and data related challenges facing organizations wishing to create a worldwide presence that are tied to the Commission's solicitation for feedback:

> **Meeting consumer expectations regarding a "fair exchange" of value.** Many services on the Internet have been provided to users at no charge in a "mostly unspoken" exchange for data collection. A prime example is location tracking, which is an essential aspect of many consumer services – consumers have little insight or control over this data and are mostly unaware of the data uses. Recent reports have highlighted that location information is often collected by Google despite tracking being turned off, and disclosure has prompted them to clarify their policy.[11] Overall, this value exchange should be made more transparent, consumers should have more granular control over collection, and they can be offered (and often are) a paid alternative if they do not wish to offer their data.
>
> **Complying with a myriad of state, federal and international regulations.** Today's privacy and data regulation world is complex, making it difficult for organizations to comply with applicable regulations in multiple jurisdictions. Smaller organizations often select the ends of the spectrum – comply with the most stringent laws on the assumption that all are adequately covered or choose to only do business in a subset of markets to restrict the range of applicable laws. Large organizations may have the resources to customize their compliance regionally, but this often adds unnecessary cost and complication, limiting opportunity and innovation. In some cases, there are even conflicts or inconsistencies between laws, further complicating the process. We believe that federal privacy and data protection regulations and legislation (as opposed to a myriad of state laws), as well as closer alignment with comparable international regulations, will help lower cost and complexity. They should be developed collaboratively as described in the next section.

Collaborative solutions for consumer protection

Additionally, we encourage the FTC to work with representatives from all impacted stakeholder groups, such as the technical community, civil society organizations, and providers, to collaboratively develop sustainable solutions to ensure users' privacy and security is upheld. The Internet Society is currently engaged in such a project in Canada[12], and we hope that it will serve as a model for the US and other nations.

For this initiative in Canada, the Internet Society has partnered with Innovation, Science and Economic Development Canada[13], CIPPIC[14], the Canadian Internet Registry Authority (CIRA)[15], and CANARIE[16] to lead a multistakeholder process to improve IoT security. So far, we have

---

[11] "AP Exclusive: Google tracks your movements, like it or not", https://apnews.com/828aefab64d4411bac257a07c1af0ecb; "APNewsBreak: Google clarifies location-tracking policy", https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211

[12] See *Canadian Multistakeholder Process: enhancing IoT security:* https://iotsecurity2018.ca/

[13] Innovation, Science and Economic Development Canada: https://www.canada.ca/en/innovation-science-economic-development.html

[14] Canadian Internet Policy and Public Interest Clinic (CIPPIC): https://cippic.ca/

[15] Canadian Internet Registry Authority (CIRA): https://cira.ca/

[16] CANARIE: https://www.canarie.ca/language/

convened and led several discussions among a group of dedicated stakeholders in Canadian technology, Internet policy, government agencies, academia, and private and non-profit sectors to identify and guide the development of recommendations for an approach to IoT policy that ensures security and consumer protection are at the heart of Internet innovation in Canada. The project has been instrumental in connecting policymakers, business, civil society, and technologists, all of whom are now working together on IoT consumer education, network resiliency, and security labelling initiatives for Canada.

Looking ahead with the FTC

To ensure that the Internet is able to continue fostering competition and opportunity, it is important that the FTC work with other stakeholders, including government agencies, to protect the Internet's key properties, such as interoperability and mutual agreement, collaboration, global reach and integrity, general purpose, innovation without requiring permission, and accessibility[17]. It is especially important to balance competition, innovation and opportunity with proper management of big data and privacy to maintain the foundation of trust in the Internet. In order to promote the Internet as an open, accessible, trustworthy resource for all, the FTC should ensure that competition policies are adapted to reflect the complexity of the modern Internet economy and enable an environment that protects consumers and encourages innovation.

The Internet Society applauds the FTC's open and inclusive approach to these hearings and encourages it to continue supporting a multistakeholder approach to Internet policy development. At the conclusion of these hearings, we hope that the FTC will continue exploring its role in these important topics by convening a working group with all impacted stakeholders to produce a set of recommendations to ensure competition and consumer protection are upheld on the Internet.

[17] The following principles are outlined in depth in the Internet Society's *Internet Invariants: What Really Matters*. Retrieved from: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-InternetInvariants-20160926-nb.pdf