Online Trust Alliance

March 30, 2016

Chairman Tom Wheeler
Federal Communications Commission
445 12th St., SW
Washington, D.C. 20554

Dear Chairman Wheeler,

In response to your fact sheet and draft Notice of Proposed Rulemaking (NPRM), regarding consumer privacy and data collection by broadband providers and wireless carriers (Providers), the Online Trust Alliance (OTA) provides the following comments.

OTA applauds the Commission's efforts to enhance consumer privacy, while recognizing the need to promote innovation. As recognized by the Commission, privacy self-regulation is failing as industry ignores the call for meaningful and persistent consumer controls. By focusing on Providers, the FCC has a unique and timely opportunity to shift control back to consumers. Unlike choosing what web sites to visit, consumers have few if any broadband options. In locations where such options are available to change Providers, the barriers and costs to change can be significant. Consumers are paying for these services and should not be also be expected to pay in perpetuity with their personal and business data.

It should be noted that data collection is not only being conducted by Providers, but also by "edge providers" including search engines, dominant analytics companies and the ad-tech industry. All parties continue to amass significant amounts of personal data. While such practices are outside of the FCC's jurisdiction, it is important that other parallel regulatory efforts are needed to help curb such practices and encourage responsible privacy practices.

As a 501(c)(3) non-profit, OTA's mission is to enhance online trust and empower users while promoting innovation and the vitality of the Internet. OTA works to educate businesses and policy makers, to drive adoption of responsible privacy practices and security standards to promote commerce and enhance the security of our nation's critical infrastructure. OTA prides itself as an active and objective participant in multi-stakeholder initiatives including fighting spam and botnets, to Internet governance, mobile security, and privacy best practices.[1] [2]

[1] OTA Anti-Botnet Initiative https://otalliance.org/resources/botnets
[2] OTA Convenes Internet Governance Leaders to Address Risks of gTLDs https://otalliance.org/news-events/press-releases/internet-governance-leaders-convene-discuss-domain-collisions

Recent examples include the formation of a multi-stakeholder botnet and Internet of Things Trust working groups. Working with over 100 organizations including input from the FCC and leading broadband providers, earlier this month OTA released an IoT Trust Framework, outlining key security, privacy and sustainability requirements.[3] Today this Framework is being embraced by a wide range of organizations providing prescriptive and actionable advice for developers and service providers. Combined these are important efforts to help enhance consumer safety and privacy. Further these efforts are critical to the resiliency of our economy and consumer trust which is the foundation of the internet and future of online services and commerce.

OTA recommends the Commission to consider the following:

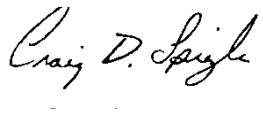
1. **Data collection for the purpose of security, fraud and related security purposes should not be restricted nor require opt-in,** providing that Providers are restricted from using such data for any other purpose, and take reasonable steps to remove any personally identifiable information when shared with third parties for threat intelligence purposes.
2. **Scope of the NPRM to be expanded to include any user data**. Increasingly businesses of all sizes, are permitting employees to utilize residential and non-traditional Internet services for work-at-home and telecommuting. As such, businesses must be afforded equal protections and considered in any rulemaking.
3. **Security** - Providers have a responsibility to take reasonable steps to help protect consumers' data and devices from harm, (e.g., malicious code or botnet activities resulting from compromise). To date many Providers have been reluctant to commit to the adoption of best practices including those published by various FCC CSRICs and other working groups. The Commission should continue to work with Providers and encourage the adoption of practices to provide consumers added transparency of their provider's security practices.[4] [5]
4. **First Party Limitations –** Data collection and use directly related to the services being provided to the user should be permitted and not required opt-in. Any usage for other purposes for un-related services should require opt-in. OTA recommends Providers annually obtain consent and opt-in for any such sharing with third parties, including unrelated affiliates or for business purposes unrelated to their current service subscriptions and services. Such a requirement would afford consumers the ability to re-evaluate their choice(s) as well as provide the service provider an opportunity to articulate to the consumer the value proposition of such activities.

[3] IoT Trust Working Group https://otalliance.org/IoT
[4] http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf
[5] See OTA Online Trust Audit and Honor Roll. Annual audit of security and privacy enhancing practices of 1,000 leading consumer facing websites https://otalliance.org/HonorRoll

5. **Respect for Do Not Track Settings (DNT)** – Providers must honor a user's browser DNT request. Reliance on cookie based controls is ineffective and does not limit data collection, or subsequent sharing and usage of user's online activities. Efforts by the interactive advertising industry have failed to provide consumers a meaningful way to curb such practices. As the industry is increasingly employing mechanisms including device finger printing and cross device tracking technologies, a universal and persistent mechanism such as DNT should be considered.
6. **Analytics** – Data collection restricted for site analytics such as measuring unique sites visitors, page views and related metrics, should be permitted and should not require user consent providing that such data is anonymous.
7. **Incentives & Competition** – Rule making should encourage and consider incentives for Providers to compete on privacy and security, starting with baseline consumer-centric notices. The Commission should consider requiring standardized privacy notices and disclosures with the goal to provide users notice on data collection, usage, sharing and retention and ability to easily compare such practices with other Providers. Another example could include discounts and incentives for consumers to share their data for marketing purposes.

In summary, OTA looks forward to working with the Commission in this and related efforts to enhance consumers' control of their data, while promoting innovation and the resiliency of our critical infrastructure.

Sincerely,



Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
https://otalliance.org
+1 425-455-7400