Online Trust Alliance

May 27, 2016

Submitted via FCC's Electronic Comment Filing System (ECFS) http://apps.fcc.gov/ecfs/

Ms. Marlene Dortch, Secretary
Federal Communications Commission
445 12th Street, SW,
Washington DC 20554.

Re: WC Docket No. 16-106
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

Dear Ms. Dortch,

In response to the FCC's Notice of Proposed Rule Making, (NPRM) to establish a set of regulations governing the data collection, use, and sharing practices of broadband Internet service providers ("Providers"), the Online Trust Alliance (OTA) submits this response. 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 drive the adoption of responsible privacy practices and security standards with the goal of promoting commerce and enhancing the security of critical infrastructure. OTA prides itself as an active and objective participant in several multi-stakeholder initiatives. Past initiatives have included fighting spam and botnets, Internet governance, mobile privacy, drones, facial recognition and IoT privacy and security.[1] [2] [3]

OTA applauds the Commission's efforts to enhance consumer privacy, while recognizing the need to promote innovation and competition. Internet access has become essential to our nation's economy and society at large. At the same time Providers have a unique role and responsibility as they have a comprehensive view of the online behavior for every home and business they serve. By focusing on Providers, the FCC has a timely opportunity to insure consumers and businesses have control over the collection, use and sharing of their personal and business data. Unlike choosing what web sites to visit, users have limited internet access options to choose from.

[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
[3] OTA IoT Trust Working Group https://otalliance.org/IoT.

Building and enhancing security and privacy into broadband services is critical to the resiliency of our economy and society. Left unchecked we risk chilling effects, disrupting business models, hampering the free exchange of ideas, and disproportionally disenfranchising segments of society.

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

In response to the NPRM, the OTA provides the following comments:

1. **Scope** - OTA recommends the scope of the NPRM be inclusive of any user data and not limited to consumer or residential services. Increasingly employees and businesses utilize residential services for work-at-home and telecommuting. Businesses and business-class services should be afforded equal protections in any rulemaking.

2. **Data Sharing and 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 re-affirm consent for any sharing with third parties, including affiliates or for business purposes unrelated to their current service(s). Such a requirement would afford consumers the ability to re-evaluate their choice(s), as well as provide the Provider an opportunity to articulate to the consumer the value proposition of the sharing of their data.[4]

3. **Privacy Notices** – To enhance transparency and encourage competitive privacy enhancing practices, it is recommended a standardized privacy notice be established, providing clear disclosure and comparability among Providers. Such notices should be designed as a layered-short notice with a standardized template which should:
    a. Define what data is collected, its purpose and how it might be shared with third parties
    b. State limitations and confidentiality requirements of any third party service provider
    c. Define data retention periods
    d. Advise customers of their opt-in and opt-out rights and provide access to an easy-to-access method for customers to provide or withdraw consent to use, disclose, or provide access to customer PI for purposes other than the provisioning of broadband services. Such methods should be persistently available and at no-cost
    e. At a minimum be easily discoverable from the site home page with a best practice to be included on the footer of every page within the site

[4] Unrelated services should include but not limited to cable TV, broadcast affiliates, advertising networks, content publishers, studios, theme parks and other services not directly tied to the delivery of broadband services.

4. **Providing Notice of Material Changes in Providers' Privacy Policies** – Users should be provided a minimum 60-day notice of any material change of a privacy policy. Such changes should provide the ability to cancel a contract, if there is no ability to opt-out of data collection, usage and sharing. Such changes should be redlined, archived and accessible from the current posted privacy policy.

5. **Data Breach Response** – Data breaches and respective data loss incidents continue to plague the public and private sectors. It is important to recognize there is no perfect security from a determined adversary; hence such rule making should not victimize the victim provided that the Provider has adopted reasonable data security practices and controls. Establishing a national breach standard for Providers provides many potential benefits. Assuming it is as robust as individual State's requirements it could relieve Providers from having to navigate the existing patchwork of State laws.

   Providers have a responsibility to take reasonable steps to help protect users' data and devices from harm, (e.g., malicious code or botnet activities resulting from compromise). To date many Providers have been reluctant to publically commit to the adoption of best practices. The Commission should encourage the adoption of best practices, and publish adoption scorecards providing users added transparency of Providers' security and privacy practices.

   OTA recommends the following:

   a. **Timing of Reporting** - In any such notification requirement to the FCC it must be recognized that complete forensics and system analysis can take weeks and in some case months to complete. Considering this fact, any such notification must recognize that the entire scope and impact may not be known or fully understood at the time of notice of an incident, and will likely require updated reports which might conflict with initial reports provided.

   b. **Customer Notifications** – It is proposed that in order to maximize the timeliness of consumer notice and reduce the risk of harm and identity theft, consumer notices be provided as soon as possible and no later than 10 business days from discovery. As it is often the case that the impact of an incident is not fully known, notifications should be provided on a rolling basis, based on the discovery of the specific records being compromised. It is conceivable additional notices would expand over months as forensics are completed and additional compromises of data stores and services are discovered. Expediting any notices reduces the window of time for data to be used maliciously and the likelihood <u>of identity theft and account compromises.</u>

      i. <u>Where compromised data or extracted data and/or device or storage media have been encrypted adhering to current NIST standards and the key not disclosed, such incidents should not</u> require notification. When there is evidence that there is no risk to the impacted user such notification should not be required.

ii. Any such disclosure of the combination of the name and password should constitute a breach and require notification, as it could lead to another online account take-over or lead to identity theft.

iii. Providing the above, notification should be required independent of any known intent of the breach or data loss incident, whether intentional, accidental, criminal or malicious in nature.

6. **Method of Notification** – Postal mail should be the primary and default form of notifications. Alternatively by email providing the following:

   a. Provider has the user's primary email account, recognizing the email account often provided to the Provider may be used infrequently or abandoned by the user.

      i. Sending email from the top level corporate domain, (typically from the web site domain of the Provider), most recognizable by the customer versus a delegated sub-domain which may be unrecognizable to the user.

      ii. All email should be authenticated, including implementation of SPF, DKIM and DMARC protocols and standards to minimize the risk of spoofing or email forgery.[5]

7. **Remedies** – While most States require identity theft monitoring service, there are currently no consistent standards. It is recommended minimum levels of service be established including but not limited to:
   a. 24 x 7 customer support. Currently many organizations provide minimum weekend or after hours support. As impacted parties may be in multiple time zones, access to support and identity theft counselors needs to be expanded including support for password reset and fraud alerting.
   b. Case worker support – Should include case worker support including a minimum number of hours per customer who has experienced an account takeover or identity theft.
   c. Multi-lingual support – As identity theft issues can be overwhelming, it is recommended support be provided in multiple languages.
   d. Support for hearing or visibility impaired – Support and resources must meet accessibility requirements.

8. **Notification to the Commission** – Notification of an incident leading to the loss of 5,000 or more records to the Commission should be made as soon as practical no later than 7 days after discovery of the breach. It is important to track such incidents for both statistical purposes and visibility of both data protection practices, internal controls and related issues.

9. **Notification to Federal Law Enforcement** – Providers should be required to notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Service) or other Law Enforcement Agencies as directed for breaches of customer PI reasonably believed to relate to more than 10,000 customers as soon as practical and no later than 7 calendar days after discovery of the

[5] Email Authentication Overview https://otalliance.org/eauth

breach, and at least 3 days before notification to the customers. The 10,000 record level the risk of inappropriately burdening law enforcement. Reporting benefits include tracking trends, providing early warnings to other Providers and business sectors.

It is understood within this short notice period, the scope and gravity of the incident will not be fully understood. In addition, information reported may be inaccurate, hampered by the short time period and inability to complete comprehensive forensics. Any such reporting requirements should anticipate these limitations. Such notices to Federal law enforcement should not be required where incidents are directly attributed to a) accidental disclosure or loss or b) employee misconduct.

As real data threat intelligence can aid the entire ecosystem, OTA recommends the FCC encourage the sharing of threat intelligence to law enforcement providing the data is confidentially held and only shared outside of law enforcement on an anonymous basis. It is acknowledged to maximize protection to both consumers and critical infrastructure with expeditious sharing, there is a risk personal information may be disclosed and such disclosure should be protected under a "safe harbor" data sharing agreement.

10. **Deep Packet Inspection (DPI)** - Should be prohibited from DPI with the exception of utilizing solely limited to fraud prevention, security purposes anti-abuse purposes. Such limitations should include the reading or scanning of any forms of electronic messaging including but not limited to email and instant messaging. Such permitted DPI data collection should be secured stored and isolated from any other use or access and destroyed after analysis.

11. **Exceptions** – a) Data collection for the purpose of security, fraud and related security purposes including such data collected through (DPI) as stated above, 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; b) Data sharing should be permitted when used for the purpose of providing email security threats and related spam reporting to ISPs, email service providers and third parties solely for the purpose to aid in the detection of blocking of malicious email, spam, cyber threats (such as phishing, malware, and botnets), and identifying and detecting network abuse; c) 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 collection is anonymous.

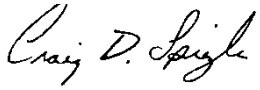
12. **Persistent Tracking Technologies Respect for Do Not Track Settings (DNT**) – Any persistent tracking should require opt-in including but not limited to the use of tracking cookies, beacons and or the use of device finger printing. As the industry is increasingly employing mechanisms including cross device tracking technologies, a universal and persistent mechanism such as DNT should be required. OTA recommends that Providers must honor a device's DNT request (or similar opt-in request) to not collect web usage or application data. Honoring such a signal should not prevent the use and data collection for site security, fraud prevention, abuse and or anonymous analytics, or sharing with third-party services providers who are legally bound to

hold such data in confidence including not sharing or using such data for any other purpose other than providing services on behalf of the Provider. Opt-out cookies were never designed to curb such data collection, and continually have been mischaracterized as doing so.

13. **Multi-Stakeholder Initiatives –** The OTA has extensive experience in both participating in and convening multi-stakeholder initiatives with the FTC, FCC, NTIA and ICANN as well as the standards community. In this capability OTA was twice appointed to the FCC CSRIC and has observed, these efforts are often dominated by the business interests of trade organizations. In addition the consensus building process unfortunately often yields a low bar diluting the impact of self-regulation and published best practices. For such efforts to succeed there must be an incentive for organizations to accept the need to change and the size of each constituency must be balanced to prevent the domination by a single group or well-funded trade groups and consortium.

In summary, OTA applauds the FCC for its thoughtful analysis of the issues and questions posed in the NPRM. Following the review of comments, OTA encourages the FCC to continue to move forward as expeditiously as possible to put in place meaningful privacy protections and control for broadband Internet users. OTA looks forward to working with the FCC and Providers in this and related efforts to enhance consumers' control of their data, while promoting innovation and the resiliency of our critical infrastructure, fostering economic growth and an open internet.

Sincerely,



Craig D. Spiezle
Executive Director and President
Online Trust Alliance
https://otalliance.org
425-455-7400