Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

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

Comments of Mozilla

Chris Riley, Head of Public Policy
Heather West, Senior Policy Manager, Americas
Stacy Martin, Senior Policy Manager, Privacy and Engagement

May 27th, 2016

TABLE OF CONTENTS

- Introduction
- Privacy and protecting usersProblem statement
- Mozilla's core approach
  - No surprises
  - User control
  - Limited data
  - Sensible settings
  - Defense in depth
- The online ecosystem
  - Broadband services and providers
  - Edge Services
  - Browsers
- A suitable privacy framework for ISPs
  - Transparency - Meaningful Notice
  - User Choice - Opt-in and opt-out
  - Data Security
  - Data Minimization
- Conclusion

Introduction

Thank you for the opportunity to submit comments regarding the Notice of Proposed Rulemaking (NPRM) on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services. Mozilla is deeply invested in creating a trusted online ecosystem both as a browser maker and also as a stakeholder in the broader ecosystem of online trust. We are deeply committed to the user - to each individual who goes online seeking access, empowerment, and opportunity.

Mozilla develops and distributes the Firefox web browser, adopted by hundreds of millions of individual Internet users around the world. Mozilla is also a foundation working to educate and empower Internet users to be the Web's makers, not just its consumers. Finally, Mozilla is a global community of technologists, thinkers, and builders who work together to promote openness, innovation and opportunity on the Web.

Through our policy and advocacy work, as a corporation, a foundation, and a global community, we focus on advancing key characteristics of the open Web, many of which are addressed in the FCC's proposed rules for broadband privacy. As the NPRM notes,[1] the protection of privacy both protects individuals and encourages use of broadband networks by building trust. Mozilla believes trust is the most important currency on the Web. We seek to build online trust so we can collectively create the Web our users want – the Web we all want.

The strength of the Web and its economy rests on a number of core building blocks that make up its foundational DNA. When these building blocks are threatened, the overall health and well-being of the Web are put at risk. Privacy is one of these building blocks. Accordingly, we are supportive of the FCC's proposed privacy rules for broadband service providers. It is important that the FCC get the details right, however, so we offer guidance based on our principles and our view of the broader Internet ecosystem as relevant to this context.

Our comments lead with a description of the problem we are collectively addressing, followed by a brief overview of Mozilla's approach to privacy. We then differentiate broadband providers as unique in the online ecosystem and briefly discuss the differences between them and edge providers. Finally, we conclude by discussing some elements of a suitable framework for privacy in broadband Internet access services.

Privacy and protecting users

Privacy means different things to different people, but people choose to make decisions about the products and services that they use based on how those companies treat their users and

[1] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC-16-39, para. 3 (rel. April 1, 2016) (*Privacy NPRM*).

their data. This is true of online services, and it is true of ISPs, to the extent that users have a meaningful choice of provider.

The FCC has statutory direction to require ISPs to protect the private information that they come into possession of in the course of providing telecommunications services. Historically, for non-Internet telecom services, the FCC has implemented its statutory obligation by requiring providers to protect and limit use of CPNI. We believe it makes sense to broaden and clarify those requirements as they apply to BIAS providers. ISPs have the potential to see a great deal of user information in the course of providing services. This centralized role means that ISPs have a heightened responsibility to protect both that information and their users.

This proceeding is timely, as ISPs continue to experiment with new ways to use subscriber data. For example, in early 2015 AT&T proposed a plan that provided discounts to users who participated in ad targeting, effectively making their plans more expensive for users who preferred stronger privacy protections.[2] Also in 2015, Verizon's unique ID headers, known as "supercookies" were reconsidered following unintended consequences and privacy concerns.[3] AT&T experimented with and then halted a similar ad-targeting program involving a unique numeric code.[4]

To the extent that an ISP treats a user simply as a target – whether for an ad, purchase, or service – that behavior undermines trust and business relationships. Requiring ISPs to adequately protect and provide transparency to their users is important to maintain trust across the ecosystem.

Mozilla's core approach

The NRPM highlights transparency, choice, and user security as the core principles for protecting user privacy.[5] We are supportive of these core principles. We similarly support the notion of a robust system to ensure that providers respect their users and provide them with adequate notice and choice. This model reflects our own approach in protecting users.

Users trust products more when companies build in transparency and user control. Earned trust can drive a virtuous cycle of adoption, while conversely, mistrust created by even just a few companies can drive a negative cycle that can damage a whole ecosystem.

---

[2] Elizabeth Dwoskin and Thomas Gryta, "AT&T Offer Data Privacy -- For a Price," Wall Street Journal (Feb 18, 2015) at http://blogs.wsj.com/digits/2015/02/18/att-offers-data-privacy-for-a-price/.
[3] Natasha Singer and Brian X. Chen, "Verizon's Mobile 'Supercookies' Seen As Threat to Privacy," The New Yorker (Jan 25, 2015), at http://www.nytimes.com/2015/01/26/technology/verizons-mobile-supercookies-seen-as-threat-to-privacy.html.
[4] *Id.*
[5] *Privacy NPRM*, para. 5.

Mozilla's Data Privacy Principles inform how we build our products and services, manage user data, and select and interact with partners – while shaping our public policy and advocacy work. [6] They were developed in 2010 and revisited in 2014, engaging a wide cross-section of our organization and inviting public input. The first two are about putting users at the center, while the last three are focused on minimizing risk to users. Each is relevant to the questions posed in the NPRM.

Mozilla's Data Privacy Principles align well with the three pillars of privacy set forth in the NPRM - transparency, choice, and security. This alignment drives our general support for the Commission's proposals in the NPRM, and shapes our analysis of the commission's proposed privacy framework.

Mozilla's five Data Privacy Principles are:

No surprises

This principle ensures that Mozilla uses and shares information in a way that is transparent and benefits the user. We provides users with meaningful notice and transparency around our privacy policies by using short and clear Privacy Notices to describe how each of our products and services receives, shares, and uses data and what the user's choices are. For us, 'no surprises' also means that our practices benefit the user, not just Mozilla. For example, collecting metrics data to improve user experience benefits both us and the user.

User control

At Mozilla, we develop products and advocate for best practices that put users in control of their data and online experiences. User control involves providing users with meaningful choice, combined with an ability to act. The other piece of this principle is advocacy - we focus not just on our own practices but on sharing best practices with the world. We want to keep striving to get better and to help others get better.

Limited data

Limited data means that we collect only what we need, de-identify data when we can and delete it if it's no longer necessary. Holding data exposes it to breach, theft, misuse, and abuse. We believe these three areas of focus - on whether the data collection is needed, whether it can be de-identified, and when it can be deleted after its utility expires - are the key to data minimization.

Sensible settings

Sensible settings is about finding the right starting point - the sweet spot between minimizing risk and maximizing user experience. When we think of sensible settings, we look for a starting

[6] Mozilla Data Privacy Principles at https://www.mozilla.org/en-US/privacy/principles/.

point that makes sense for most users, with user control options to empower the user to make changes.

Defense in depth

Defense in depth is a security concept used to describe multi-layered protections. For us, this begins with our open source code (available to be evaluated and studied by third parties), and our transparency in the event of security issues promoting greater verifiability and trust by the public.

The online ecosystem

Some parties in this proceeding will undoubtedly strive to tangle the Commission's proposals in rhetoric comparing ISPs to other actors in the online ecosystem. But each of our guiding principles - and indeed, transparency, control, and security broadly - manifests differently for various online actors, so regulatory frameworks for each of them must correspondingly be examined separately (to say nothing of inherent limits on statutory authority). In other words, for the ecosystem to remain healthy, all players must respect user privacy, but implementation in practice is extremely different based on the technical features of the player, including but not limited to their access to user information. In particular, we feel it's important to understand the key differences between ISPs and edge services.

Broadband services and providers

As noted in the NPRM, broadband providers - also called ISPs - are "the most important and extensive conduits of consumer
information and thus have access to very sensitive and very personal information."[7] The kinds of data they have access to, combined with the relative difficulty of switching ISPs compared to the ease with which a consumer can switch edge service providers or applications, differentiates the role they play online in an important way.

Broadband providers are the gateway to online information and services. All of a user's network traffic goes through their ISP, which means they have unfettered access to usage patterns and metadata. Usage patterns and metadata can be as revealing, or in some ways even more revealing, than content. Furthermore, users typically don't think about the potential for disclosure of private information that can come from metadata. For example, even when a user is accessing a Web site protected by HTTPS, the ISP is able (along with other devices on the same local network) to identify the Web site being visited, though not the individual page.

It's also important to look at what data the ISPs can connect usage patterns and metadata to. Because these are paid services, they have the subscriber's name, address, phone number and billing history. The combination gives ISPs a very unique, detailed and comprehensive view of

[7] *Privacy NPRM*, para. 3.

their users that can be used to profile them in ways that are commercially lucrative. What's more, none of this information is optional for the user to provide, making it especially important to implement strong privacy protections for the user. In sum, we agree with the Commission that ISPs are different and should be treated differently.

Edge Services

Edge services are the services that travel (ultimately) over broadband provider networks in order to reach the end user. That includes, for example, Google, Facebook, and Verizon's non-ISP services, as well as all websites on the Internet. Regulatory oversight for privacy practices of edge services generally lies with the Federal Trade Commission rather than the FCC.

Certainly, edge providers have access to significant information about users. Some use explicit tracking systems to collect information on Internet activity above and beyond direct, first-party interactions with the service. Others confine their data collection to information voluntarily provided by the user in setting up and continuing service.

But their access to data differs technically from that of ISPs in two significant ways: First, modern-day edge providers often offer thorough privacy interfaces to enable reasonably fine-grained control over collection and use of data. Second, users have some technical potential, using add-ons or features such as Firefox's tracking protection in Private Browsing mode, to block edge providers from tracking and collecting information about them. These services are designed to be easy-to-use and to improve, rather than degrade, technical performance.

This second point is particularly illustrative as a point of contrast to the relationship between a user and an ISP. Greater lengths are needed to mask metadata and usage patterns from an ISP. A VPN service or powerful anonymity service such as Tor is required to offer even partial protection, and such services by engineering necessity degrade performance by increasing latency (as they must first redirect traffic to an intermediate location in order to hide the final destination from the ISP).

A suitable privacy framework for ISPs

The NPRM proposes to require ISPs to provide transparency and security and give consumers control over what personal information is used and shared. We recognize that such uses of user data have been emerging as a promising source of new revenue streams for ISPs, and our objective is not to prevent them. But they must be offered transparently and with meaningful choice to serve the public good. In too many cases, we worry that such uses are not transparent, leaving users in the dark about what if any benefits they receive as well as what price they are paying with their data. And too often they are not optional, leaving users powerless to shape their online experience.

In this proceeding, the Commission has an opportunity to ensure alignment of user interests with business incentives, and to create a constructive feedback loop so that positive user experiences are rewarded with better business outcomes.

With that goal in mind, and in line with Mozilla's privacy principles, we would like to comment on each of the three pillars raised in the NPRM - transparency, user choice, and security - as well as on a related topic, data minimization.

Transparency - Meaningful Notice

The NPRM seeks comment on best practices for providing users with meaningful notice and transparency around privacy policies.[8]

We strongly support the requirement that users be given meaningful notice. This is consistent with Mozilla's first data privacy principle of no surprises. Our users and our community have told us – through surveys, comments and emails – that transparency and control matter to them. They want to know what is happening with their data; they want to control what data is shared, understand how their data is used and what they get for that exchange. They are willing to engage in the value exchange and allow their data to be used if they understand what happens next. We believe meaningful notice contributes to trust which in turn increases the health of the online ecosystem.

We support the Commission's proposal for disclosure requirements for ISPs that are consistent with using and sharing information in a way that is transparent, including timely and persistent notice. In general, the proposed practices in the NPRM are consistent with best practices in our industry.

User Choice - Opt-in and opt-out

The NPRM opens a discussion of customer approval requirements, under the pillar of user choice, with the goal of enabling the user to decide how their information is used.[9] The NPRM proposes a three tiered approach to choice that recognizes three categories of approval based on allowing implied consent for necessary services, opt-out for marketing and opt-in for other data uses which may be unexpected by the user.

Generally, we support the proposed framework. We would caution the Commission to interpret narrowly those uses that may be "expected", and not to accept the provision of either a detailed legal document or a flimsy disposable glossy flier, handed out at the initiation of service, as sufficient to create user expectations of use of their personal data sufficient to convert from an opt-in to an opt-out requirement. In both cases - those uses that are opt-out and opt-in - users should ideally have an easy-to-access, 24/7 online portal to view their current choices and make

[8] *Privacy NPRM*, para. 83.
[9] *Privacy NPRM,* para. 106.

changes, and should be able to make such changes over the ISP's customer service structures such as by telephone, email, and chat. Additionally, users should be able to change their minds at any point in time, and should not be locked into a decision on opt-out or opt-in for any longer than technically necessary to change the system's behavior.

Data Security

The NPRM seeks comment on protecting users against the unauthorized disclosure of their information.[10] It also asks for information about how broadband providers can ensure that user data is secure, and what recourse users deserve when it is compromised.

Mozilla generally supports the use of increased security measures such as multi-factor authentication and password protection. Multi-factor authentication is broadly used to protect financial, personal, and other information stored in online accounts. This greatly enhances online security for this information, and could be highly useful in many contexts related to ISP collection and use of user data.

Rather than specifying particular methods by which a broadband provider might protect user information, we believe the final rule should require that broadband providers use industry-standard or better security practices.

Data Minimization

The NPRM also seeks comment on whether there are other data security requirements that the Commission should adopt, such as data minimization, retention, and destruction requirements.[11]

Limited data is one of Mozilla's core data privacy principles mentioned earlier and Mozilla believes these three areas of focus - determining whether the data collection is needed, whether it can be de-identified, and when it can be deleted after its utility expires - create the framework needed to build trust and reduce risk. Users are much less likely to use products and services they don't trust. Once trust is lost, it is hard - and sometimes impossible - to regain. As with transparency and choice, data minimization can help can help build a trusted ecosystem.

In addition to building trust, data minimization reduces risk. Every additional byte stored increases operating costs and breach risks. We use limited data as a starting point for our own decisions about data at Mozilla and we share our data principles in an effort to evangelize and advocate for better data stewardship and management. We believe smart data practices are the key to data minimization.

---

[10] *Privacy NPRM*, para. 167.
[11] *Privacy NPRM*, paras. 22, 169.

Conclusion

Thank you for soliciting comment on important privacy questions for broadband providers. These providers serve as users' gateway to the Internet and hold a privileged place in the ecosystem, placing greater importance on the protections that they provide to users. Mozilla generally supports the spirit of the proposed rules as described in the NPRM. We commend the FCC for its commitment to finding the best approach to protecting consumers' privacy when they use broadband services and to upholding the principles of transparency, choice, and security.