A Submission from Cloudflare, Inc., in response to

"Request for Comment on Developing the Administration's Approach to Consumer Privacy" Docket No. 180821780–8780–01

A Notice by the National Telecommunications and Information Administration on September 26, 2018

November 6, 2018

Cloudflare welcomes the National Telecommunications and Information Administration (NTIA)'s efforts to explore the issue of consumer data privacy, and views the Request for Comment (RFC) as being a timely and important initiative. The RFC is a thoughtful and thorough document, and the emphasis on a risk and outcome-based approach suggests a process and framework that will be comprehensive, thoughtful, and not reactionary. Cloudflare submits the following comments, which will address how we believe privacy protection outcomes can best be achieved, along with a prioritization of goals.

Overall, Cloudflare would urge the NTIA and Administration to adopt an approach that is flexible and responsive to the dynamic nature of the technology sector in particular, while also being technology neutral, and one that allows for necessary cybersecurity research. We encourage regulators to be mindful of the disproportionate impact data protection laws can have on small or new businesses that may not be able to afford the cost of compliance nor have significant available resources on hand. Small businesses who work with less sensitive data should be allowed to identify solutions tailored to their business and resource capabilities.

NTIA has an opportunity to lay out a vision of privacy protection that embraces both the rights of consumers and the encouragement of innovation, and restores the leadership role of the United States on these critical issues. We would also support Federal legislation that serves the same goals. As a US-based company, we believe it is essential that the US government establishes its commitment to a comprehensive and robust privacy regime, congruent with privacy regulations around the world.

Background on Cloudflare

Cloudflare's mission is to help build a better internet, which means many things to us as a company. It means we work hard to make Internet properties faster, help

make the Internet more reliable, support new Internet standards and protocols, make services accessible to everyone and make it more difficult for malicious actors to perpetrate cyber attacks. Our mission drives us to increase value for our community, while decreasing their costs. The ideals at the heart of all of these efforts are security, trust, safety, and inclusivity.

As we put these ideals into action, privacy and transparency are critical. Entities with web properties sign up for our services to speed up access to their sites and keep themselves secure and online. Today, we serve more than 10 million websites world wide, ranging from individual blogs to small businesses to large Fortune 500 companies. We operate a global network that transmits as much as 10% of all global internet requests, speeding up those requests by 2x, on average.

We don't just talk about how important privacy is, we develop products that are designed to provide both our customers and their end users with additional control over their private information. For example, our customers -- both those who pay for our services and those who use use our services for free -- benefit from free SSL certificates, ensuring that every website on Cloudflare can create an encrypted connection between the website and the browser and preventing a user's personal information from being exposed. We also support DNSSEC, which uses signed certificates to prevent hijacking of DNS look-ups. Cloudflare recently announced that we would be supporting automatic DNSSEC, where registries scan and upload DS keys from Cloudflare, enabling increased usage of DNSSEC and additional security on the net. This year we also launched a product called Spectrum, which allows us to provide security and encryption for all TCP traffic rather than solely HTTP traffic.

We have also created products that make web browsing more private. For example, when browsing the web, there are a variety of ways that a user's personal data may be exposed, allowing third parties to snoop on their browsing history or network providers to collect and sell their data. To enable our users to take control over who is viewing their personal browsing information, this year Cloudflare launched 1.1.1.1, a privacy-focused DNS resolver. Our resolver encrypts DNS requests, ensuring that third parties between the user and the DNS servers cannot see the user's information in plain text. To rectify the fact that a third party might not know exactly which user is accessing websites, but will know what website is being accessed and may be able to trace requests, Cloudflare introduced encrypted Server Name Identification (SNI), which encrypts the URL of the website a user is

accessing. Mozilla has recently added eSNI functionality for testing on Firefox Nightly.

These services are our product; our users' personal data are not. We keep our users' personal information personal and private. We will not sell, rent, share, or otherwise disclose that personal information to anyone, except as necessary to provide our services and, where appropriate, we provide users notice and the opportunity to consent.

In order to earn the trust of our customers, we couple our commitment to privacy with a commitment to transparency. To that end, we have posted our privacy policy on Github, so our customers can see when and how we might change it. We know our customers are savvy, privacy conscious and security-minded, and we want to make sure they have tools to hold us accountable. We are also extremely transparent in our communication about our own mistakes and failures. We keep a very active blog to share details of new products and ideas, but we also regularly share post-mortems when we fall short of our own expectations. We have detailed analyses of network outages, of DNS updates gone wrong, and of tough policy decisions. We believe that trust can only be earned when we are honest with our users.

OUTCOMES

The outcomes laid out in this RFC are very much in keeping with our own practices. We are reassured to see a combination of the OECD privacy principles and the Fair Information Practice Principles (FIPPs) used as the framework here, keeping this in line with Europe's General Data Protection Regulation (GDPR), a structure most companies have already begun implementing.

1) *Transparency*. We have strived to write our own privacy policy in plain English, but we recognize that customers do not always read or understand privacy policies. While we support finding innovative ways to communicate with customers about the use of their data, we would urge a non-prescriptive approach. A contextual strategy for privacy notices would ensure flexibility, a user-centric approach, and the ability to comply with other laws. Unless a Federal law offers preemption, we must still comply with local laws that require a privacy policy to be shown when personal information is first gathered.

2) *Control.* Users need to be able to easily withdraw consent to the processing of their personal information. We implemented such a mechanism to comply with the GDPR but would caution that any requirement should be technology neutral. Particular requirements regarding design or functionality may make sense in some contexts, but might be unworkable in others. Mandating particular placement of buttons or controls that look a certain way or follow a particular flow run the risk of tying the hands of innovators. Requirements that don't take into account new discoveries in user experience risk robbing consumers of control and choice regarding the use of their personal information.

3) *Reasonable Minimization.* Cloudflare limits the collection of personal data to that data that is required for operation, which is an approach that is consistent with our business model and approach to security. Recognizing that standards relating to the appropriate collection of data is one of the key friction points when it comes to privacy protection, we would recommend that NTIA provide additional context for what reasonable minimization means for different types of companies and business models. For example, although a vast amount of traffic runs across Cloudflare's networks, we processes a very limited amount of customer personal data as a data controller. Traffic data that we process on behalf of our customers only contains minimal "personal data" in the form of IP addresses. When considering the minimization of personal data, we balance the utility of this information for delivering the security services our customers expect with meeting privacy best practices. We therefore believe that any data minimization should take into account the level of sensitivity of the data, the purpose of use and the reasonable expectations (and instructions) of the user. "Reasonable" minimization could and should look very different for different types of businesses, and should be based, at least in part, on risk assessments.

4) *Security.* Security is core to our business, and we believe it can play an important role in improving privacy protections. As a principle, we agree that organizations that collect data should take all reasonable measures to secure that data. There are many different technological tools available to improve security, and we believe that companies should be incentivized to make use of them. For example, companies should be encouraged to use security best practices, advanced state-of-the-art technologies such as encryption, and anonymization/pseudonymization techniques. And where such incentives fail

to persuade companies to implement levels of security appropriate to protect the privacy of their users' data, companies should be held accountable.

5) *Access and Correction*. We believe individuals should have a right to access and maintain the accuracy of their personal data, and that customers should be able to ask for their data to be deleted. Indeed, we have implemented mechanisms to allow individuals on our network to exercise these rights. We also support the way in which the GDPR allows data controllers to respond to data access requests by providing categories of data collected and processed. We believe that companies should have the right to confirm requesting individuals' identities and that data processors should have the ability to reasonably reject deletion requests, for example, if an individual continues to use a service and the use of their personal data is necessary for the provision of that service. Giving companies the opportunity to reject deletion requests in deference to companies' legitimate interests to process the data to allow for continuity of service - or for other legitimate reasons such as billing - is important.

6) *Risk Management.* Organizations should use appropriate measures to secure the data that they have in meaningful and proportionate ways. Cloudflare fully supports the use of a risk-management framework and appreciates the Administration's commitment to providing companies the flexibility to make decisions based on the context of their individual businesses. We support a common baseline, with flexibility to add additional features on top, conditional on the use and type of data an organization collects.

   Government can play a positive role in risk management by taking steps to reduce the potential impact of exposure of information. Collection of personal data poses a more significant risk to consumers if that same personal data can be misused to assume someone's identity or affect their access to goods and services. A leak of social security numbers, for example, is problematic because social security numbers have become the way in which to access sensitive documents, like financial, health and education records. Rethinking this model, and potentially developing new ways of addressing digital identity, could go along way to reducing privacy risk for consumers.

7) *Accountability.* Accountability is essential to raising the bar on consumer privacy protections. We are unclear, however, how this will work in practice. While this seems like an obvious fit for the FTC, they will need significantly more resources before they can be expected to effectively enforce new privacy standards. This process is evidence that consumer privacy is a high priority for this administration, so we would hope that they would put resources and effort behind an enforcement body.

   Companies have a role to play in holding themselves accountable by providing transparency to their users. Cloudflare publishes biannual transparency reports about the governmental requests we have received to disclose information about our customers. It is also our company policy to inform our customers when requests to access their data have been made, absent any legal instruction to the contrary.

   We also take steps to provide information about the use of the Internet in a ways that can increase accountability. We announced in March of this year, for example, that we had created a free and open certificate transparency log, as well as a dashboard for exploring the certificate transparency ecosystem. Certificates are put onto an ordered list, and audited regularly. This effort is designed to provide additional public information about certificate authorities' use of Public Key Infrastructure (PKI) to keep log operators honest. Malicious actors can mis-use certificates to impersonate websites and target individuals by directing them elsewhere. Making all certificates public will expose the mis-issued certificates.

GOALS

Harmonize the regulatory landscape

In an increasingly globalized world, consumers and companies deserve a clear, comprehensive privacy framework that is interoperable with global legal schemes, and one that engenders trust and clarity. A patchwork of regulations across the world leads to high compliance costs and productivity losses, a significant administrative burden for companies, especially for startups. This could be seen as a barrier to market entry unless there is some flexibility for smaller businesses. Europe's pursuit of extra-territorial jurisdiction under GDPR has led to other countries pursuing their own independent efforts to adopt a similar approach. California's privacy bill brings up similar concerns within the United States. A unified

standard in the United States is essential for small and medium enterprises to continue to innovate and thrive.

For US companies with significant operations in Europe, a chief concern is whether any US law would render the US an "adequate" jurisdiction in GDPR parlance. We are concerned that a voluntary, guidelines-based approach in the US would not meet the standards and expectations of European data protection regulators. If we do see a federal privacy law in the US, there must, at a minimum, be meaningful enforcement mechanisms that meet global data protection law standards.

Employ a risk- and outcome-based approach

A risk-based approach, similar to NIST's cybersecurity framework, will be a good starting point for a privacy overhaul. Graduated responsibility based on the sensitivity of data, and the way in which the data is processed and used is important. Companies should be incentivised to use state of the art technologies in protecting the personal data of their users. Were there to be a breach, a company's demonstrated efforts in using strong data protection mechanisms and techniques should be taken into consideration. Just as privacy mechanisms are deployed in proportion to the scale and scope of info the company is handling, enforcement should take context into consideration. Companies should be motivated to use privacy by design, and encouraged to deploy innovation in the area of privacy protection.

There should be some effort to enforce penalties for organizations that use data in ways that are clearly inappropriate, however "inappropriate" may be defined in a given context. It could be that an organization uses data in a way that is contrary to the user's expectations based on the original stated purpose for why it was collected. Privacy comes down to trust, and many of the recent news stories where companies have used data for unexpected things have caught our attention because consumer trust was betrayed. In some cases that was because the data was collected for one purpose, and used for another.

Incentivize privacy research

We fully support incentives by the US government to support privacy research. We agree that we need to incentivize technology development that increases

privacy and security, and we also want to ensure that the government doesn't hinder technology developments that improve privacy and security.

Encryption is key to privacy on the internet, and any government-mandated encryption back doors would be highly concerning as it undermines protections. Moreover, in the wake of discussions around proposed content filtering initiatives in the EU, we would urge governments to consider potential resultant privacy weaknesses. Some incentives towards privacy research should be dedicated to analyzing the costs and benefits of government mandates that weaken security.

Additional Considerations

The most important goal of any US privacy effort should be to bolster and strengthen the ability of US companies to operate globally. The US government should use all of the tools at hand, including trade agreements, to ensure that data is able to flow freely across borders and that our rules are interoperable with other laws and regulations around the world.

The Federal government could explore a sufficiency scheme, where companies under a certain size, or with a presence below a certain threshold in another country, could be free from the burden of answering complaints in that jurisdiction. The country could then file the complaint with the FTC and rely on the FTC to take appropriate action. To allow small and medium enterprises to answer complaints in front of a single body, regardless of the jurisdiction where the breach occurred would go a long way towards reducing the burden of compliance.

The second key piece of any US effort on data privacy is to ensure that it is has the ability to evolve and flex over time. This can be achieved by using technology neutral language and leveraging industry advisory groups and technical experts for ongoing guidance.

Finally, we would ask that the definition of personal data be clarified. Different definitions of sensitive personal information, personally identifiable information, and information that is able to be attributed to an individual are all being used across various privacy frameworks. We would ask for a US effort that clarifies this language, as well as making a clear distinction between natural persons and legal persons.

Conclusion

Cloudflare appreciates NTIA's solicitation of diverse set of views on consumer privacy. We look forward to continuing to engage with NTIA on privacy and consumer protection.

Sincerely,

Erica Fox
Senior Manager, Public Policy
Cloudflare
1401 K St. NW, Suite 875
Washington, DC 20005