A Submission from Cloudflare, Inc., in response to

"Request for Information on Developing a Privacy Framework" Docket No. 181101997-8997-01

A Notice by the National Institute of Standards and Technology on November 14, 2018

December 7, 2018

Cloudflare appreciates the opportunity to comment on the National Institute of Standards and Technology (NIST) Request For Information (RFI) on "Developing a Privacy Framework." This RFI asks a number of substantive questions, and we hope the exercise will result in a useful sharing of best practices amongst stakeholders. Cloudflare submits the following comments, which will address our own experience in measuring privacy risk and how we believe incentives need to be realigned cross-sectorally. Our response also details our questions and concerns regarding the development of a framework.

NIST has an opportunity to propose a standard for use by businesses that fosters innovation while encouraging consumer protection, and one that clarifies the global rules of the road on privacy for businesses. We have publicly supported Federal legislation that serves those same goals and would welcome NIST's timely contribution to this effort.

Background on Cloudflare

Cloudflare's mission is to help build a better internet. At the time of our founding in 2010, that meant making available to all entities security services which previously were available only to the largest companies. These days, we work hard to make Internet properties run faster, help make the core Internet more reliable, support new Internet standards and protocols, and make it more difficult for malicious actors to carry out cyber attacks. Our mission drives us to constantly innovate new ways to protect our community of users, while decreasing their overhead. The ideals behind these efforts are security, trust, safety, and inclusivity.

Privacy and transparency are crucial in realizing these ideals. Businesses and individuals with web properties sign up for our services to keep themselves secure and online and to speed up access to their sites. Today, we operate a global network that speeds up internet requests and serves more than 12 million

websites world wide, ranging from individual blogs to small businesses to large Fortune 500 companies.

Our commitment to privacy is evident in our actions, not just our words. We believe in privacy by design. In service to that we have created products that make web browsing more private. For example, when browsing the web, a user's personal data may be exposed, allowing malicious actors to snoop on their browsing history or network providers to collect and sell their data. To enable our users to take control over who has access to 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 who sit between the user and the DNS servers cannot see the user's request 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.

We also develop products that provide both our customers and their end users control over their personal information. For example, our customers -- both those who pay for our services and those who 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 the hijacking of DNS look-ups. Cloudflare recently announced that we would be supporting automatic DNSSEC, where registries scan and upload DNS 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.

These services are our product; our users' personal data are not. We believe our users' personal information is personal and private, and we keep it that way. We will not sell, rent, share, or otherwise disclose that personal information to any third parties, except as necessary to provide our services or as required by law, and we provide users clear notice and the opportunity to consent.

Trust is paramount to a cybersecurity company. To maintain our customers' trust, we try to be very transparent about our actions and our decisions. As part of

our commitment to accountability, we have posted our privacy policy on Github so our customers can see the changes we have made over the years. We know our customers are savvy, privacy conscious and security-minded, and we want to make sure they have the tools to hold us accountable. We also endeavor to be transparent in our communication about our own mistakes and failures. We keep an active blog that shares details of new products and ideas and also regularly shares post-mortems of any incidents. We have detailed analyses of network outages, of DNS updates gone wrong, and of tough policy decisions. Building trust is an ongoing process, and we are committed to doing the work.

Areas for more research

We agree with NIST's recognition that there may be aspects of consumer privacy which require further research. We would like to see research around rethinking digital identities. Theft of social security numbers, for example, is problematic because social security numbers have become the way in which individuals in the US access sensitive documents like financial, health and education records. This data becomes far more sensitive when it can be misused to impersonate an individual. Yet we rely on it to verify identity all over the Internet. Reconsidering this model, and developing new methods of digital identity, could seriously reduce privacy risks for consumers online. For an effort like this to be successful, it would need to be widely adopted and we believe that NIST would be uniquely positioned to explore and initiate such a project.

We would also urge NIST to take up research on the ways technical measures like encryption benefit user privacy. We rely on encryption to build our cybersecurity products and keep our customers' data secure, and we believe that it is key to privacy on the internet. As governments continue to debate the merits of requiring companies to build backdoors into their products, we would all benefit from fact-based research into the costs and benefits of breaking encryption.

Organizational Considerations

Challenges in a cross-sectoral approach

We see three distinct challenges in developing a cross-sectoral framework for privacy. The first challenge we can see is the different definitions of personal data that the existing consumer privacy regimes employ. We would like to see a framework with a clear definition, making a distinction between natural persons and legal persons, while acknowledging the different definitions employed in Europe's General Data Protection Regulation (GDPR) and the California Consumer

Privacy Act (CCPA). We believe this framework could serve as a resource for businesses struggling to understand how the different definitions apply to their products and services, and would be particularly helpful for those businesses that operate across borders.

A second concern is that this framework is able to be rationalized with existing sector-specific US privacy laws. We want to understand how this privacy framework will relate to the Health Insurance Portability and Accountability Act (HIPPA), the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA) and others. Will it carve those types of data out? Will it apply to them? And should it? We believe that this process should help companies understand and smooth out their responses to our existing patchwork of laws.

Lastly, we are concerned about how sensitivity of the same data may differ dramatically across industries and uses. Context is important when determining the sensitivity of data, and if we employ a risk-based framework cross-sectorally, it will likely look very different for each sector. How do we create a framework that allows companies the flexibility to create risk-based approaches targeted to their own data privacy needs, without creating a watered-down standard? If this framework is to accomplish the goals as laid out, it must inspire confidence in users and governments around the world.

Incorporating privacy into our risk management framework

Cloudflare has fully incorporated privacy into our risk management framework. As a cybersecurity company, we know we have to practice what we preach. As such, privacy risk has been seamlessly integrated into our risk assessments from the outset. Maintaining the trust of our customers and users is important to our business and also essential in service to our ideals. But how do we build in incentives in a privacy framework for companies who lack the inherent motivation and reputational considerations? We would like to see this framework explore ways to incentivize all entities to consider privacy protections and to adopt privacy-by-design.

Current procedures for managing risk

We have updated our data handling processes and procedures in light of new global privacy regulations such as Europe's General Data Protection Regulation (GDPR). Standards like PCI compliance (the Payment Card Industry Data Security Standard) and SOC 2 (Service Organization Control 2) compliance require us to undergo thorough risk assessments, which we have adapted to meet each new

requirement. These are ongoing, critical elements of our privacy and security programs. We also conduct assessments that identify risk in our regular data privacy assessments. And finally, we are dedicated to privacy by design. We emphasize these principles in our product launch checklists, and work to ensure that privacy is built into each product before it is released.

Minimum attributes for a privacy framework

At minimum, we believe that NIST's privacy framework should be responsive to the dynamic nature of the technology sector, non-prescriptive, and flexible. We would urge that it be technology neutral, and make allowances for necessary cybersecurity research. We also believe that it is essential that any framework be compatible with other privacy approaches around the globe, including GDPR, CCPA, privacy laws in Australia, Brazil, and China, as well as the other industry-specific privacy laws in the US, including COPPA, FERPA, and HIPPA.

On that last point, we believe that NIST's privacy framework could serve as an ideal vehicle to bring analysis of how all of the competing privacy standards together fit together. Small and emerging companies find it challenging to work with a patchwork of privacy rules depending on the type of data and jurisdiction in which they operate. An assortment of regulations across the world leads to high compliance costs and productivity losses, a significant administrative burden for companies, especially for startups. If NIST could map how their privacy framework would help address compliance with privacy regulations around the world, it would give these companies meaningful analysis and advice on how to structure their practices to meet all of their competing obligations. This would save companies from duplicating already scarce resources and provide clarity from a trusted authority.

International implications of a privacy framework

In an increasingly globalized world, consumers and companies deserve a clear, comprehensive privacy framework that is interoperable with global legal schemes and that engenders trust and clarity. 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 would consider NIST's framework to be a helpful step in signalling to the EU that the US is serious about consumer privacy protections, and taking meaningful measures to ensure they are put in place.

Structuring the Privacy Framework

How we manage privacy risk

Cloudflare structures our privacy risk program around controls established by the various regulatory schemes to which we are subject. As we collect data, or as data transits our network, we map the data flows against regulatory controls. When a product team considers using personal data, we evaluate the contemplated use or collection of data measure those requests against the controls in GDPR and similar regulations. Owing to the shared principles at the heart of the GDPR, FIPPs and other regulatory schemes, it would be fair to say that our privacy risk management structure incorporates FIPPS.

Our preferred construct for a privacy framework

The most important part of the choosing of an organizing construct for NIST's privacy framework is ensuring that it follows the same constructs as the GDPR, CCPA and the other regimes mentioned earlier. GDPR's founding seven principles of lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and accountability are a good place to start. These principles can be found in different iterations in many of the new consumer privacy laws and other bills that have been proposed.

Specific Privacy Practices

We encrypt our data, and follow best practices as well as legal requirements when handling customer data. We map the data through its lifecycle and -- except the data we are legally obligated to keep -- delete personal data according to the principles of data minimization and the right of a data subject to object to processing. We also manage data responsibly, instituting access controls, so that only the employees who need to use the data have access to it. We are also in the process of instituting multiple regular auditing processes to hold ourselves accountable.

Practices we see as most critical for protecting an individual's privacy

Before we determine which privacy practices are most critical for protecting data, we think it might be useful to take a step back. We should understand what NIST's privacy framework is seeking to protect. It might be useful to lay out our priorities when it comes to protecting data, so that we can fully understand how we determine what and who merits protection.

For example, as a company largely operating in the business-to-business space, we see pseudonymization and/or anonymization of customer data as integral to protecting consumer privacy. Ad-supported businesses, on the other hand might prefer to see granular user choice options so people can personalize the kinds of ads they see . Some privacy regimes like Brazil's data privacy law treats pseudonymized data as personal data, which could have a seriously detrimental effect on cybersecurity research. Having the freedom to use pseudonymized data to draw security conclusions is an essential part of the research we do, and the security of the Internet.

Lastly, we believe that strong encryption is key to privacy on the internet, and any government-mandated encryption back doors would be highly concerning. In the wake of discussions around proposed content filtering initiatives in the EU, and the recently-passed Australian access law, we are growing increasingly concerned that governments are introducing vulnerabilities at a time when there has been an unprecedented volume of state-sponsored cybercrime. We would urge governments to consider the potential resultant privacy weaknesses they would introduce when forcing companies to break encryption. Some privacy research funds should be dedicated to analyzing the costs and benefits of government mandates that weaken security.

Whether some of these practices are inapplicable for particular sectors or environments

There are some privacy practices that are critical for ensuring user and consumer privacy. These practices do not always apply to business-to-business companies, or infrastructure companies like ours. For example, while we support consumer choice and consent as an effective method for providing consumers with privacy protections, in a business-to-business model, our customers -- not us -- have the direct relationship with their individual end users. We cannot provide our customer's end users with an ability to opt out of our customer's data collection.

Therefore, we emphasize our support for a framework that proposes a common baseline, with flexibility to add additional features on top, conditional on the use and type of data an organization collects. A risk-based approach, similar to NIST's cybersecurity framework, would be a good model. Graduated responsibility based on the sensitivity of data, and the way in which the data is processed and used would be an option. Companies should be incentivised to employ state of the art technologies when protecting the personal data of their users. In that case, were there to be a breach, a company's clear efforts to use strong data protection

methods should be taken into consideration. Just as privacy mechanisms are deployed in proportion to the scale and scope of data 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 their privacy protection.

Further, we would consider there to be serious implementation challenges in any framework that suggests retroactive anonymization or deletion of specific PII elements that may have been captured. Anonymization and encryption can be technically challenging, and not every company has the resources to accomplish this, particularly if it is backward-looking. Workforce capability should be a consideration in any proposal, particularly considering the unique challenges facing small or emerging businesses.

Whether these practices are relevant to iOT and AI

In short, absolutely. We are confident that the rapid growth in both areas and the quantity of personal data collected and processed will require serious privacy protections. The value of a NIST standard is that it can be drafted to take into consideration the current challenges with unprotected iOT devices, but also allow for AI considerations to evolve. Additions and corrections can be made to a framework as iOT companies commit to strengthening their security practices and committing to privacy. The policy conversations around artificial intelligence are still in their infancy, and while we know there must be controls, we do not yet know the full extent of what is needed. This framework can leave space for that, without being proscriptive.

Conclusion

Cloudflare appreciates NIST's specific and comprehensive questions, and the breadth of expert opinion they will generate for the field. We look forward to continuing to engage with NIST on privacy and consumer protection as this process moves forward.

Sincerely,

Erica Fox
Senior Manager, Public Policy
Cloudflare