A Submission from Cloudflare, Inc., in response to

"International Internet policy priorities", Docket number 180124068-8068-01

A Notice by the National Telecommunications and Information Administration, issued on May 31, 2018

July 17, 2018

Cloudflare welcomes the opportunity to comment on the international Internet policy priorities of the National Telecommunications and Information Administration (NTIA). We support NTIA's efforts to protect and promote an open and interoperable internet and advocate for the free flow of data. NTIA's work on international Internet policy is critical to maintaining an open and vibrant Internet that furthers economic growth and innovation.

Background on Cloudflare

Cloudflare is an Internet performance and security company that is on a mission to help build a better Internet. Our global network of 151 points of presence in 74 countries powers more than 10 trillion requests per month, which is nearly 10 percent of all Internet requests for more than 2.5 billion people worldwide. Because of our global presence and the amount of traffic that flows over our networks, we are well positioned to comment on the challenges faced by Internet infrastructure companies around the world.

Setting Priorities

The NTIA request for comment is divided into four categories: (1) the free flow of information and jurisdiction, (2) the multistakeholder approach to Internet governance, (3) privacy and security, and (4) emerging technology and trends. The questions posed on all of these topics highlight the challenges currently faced by the Internet.

Cloudflare believes there is one basic principle from which all of NTIA's priorities should flow: the Internet must continue to operate around the world. If the public loses confidence in the integrity and reliability of the Internet, the Internet will no longer be able to fulfill its social and economic promise. To that end, we believe NTIA should encourage:

(1) The development and support of norms that protect against attempts to use the core technical workings of the Internet-- like DNS, transmission systems and methods for cryptographic security and identity-- to further nation-specific priorities that seek to fragment the Internet.

(2) The development, deployment and adoption of technology that improves the security and privacy of all information on the path of Internet transmission.

(3) Participation in intergovernmental and multistakeholder fora that help develop consensus positions on how to address access to data and restrictions on content, preventing conflicting requirements across countries.

(4) The adoption of policies that encourage interconnection and drive Internet access costs down.

Additional information on each of the specific categories is addressed separately, below.

I. The Free Flow of Information and Jurisdiction

The last few years have presented significant challenges to the free flow of information online, with a variety of countries imposing measures blocking Internet access, mandating data localization, requiring or encouraging Internet platforms to remove or block perceived harmful content, restricting the use of secure technologies, and limiting interconnection through fees.

As an Internet infrastructure company, Cloudflare is particularly concerned with efforts to address problematic content that -- either intentionally or unintentionally -- affect the technical workings of the Internet. We believe that the roles and responsibilities of infrastructure providers in ensuring the free flow of information online differ from those of platforms that manipulate or organize content.

In order to encourage the free flow of information online, NTIA should continue to support laws which limit the liability of intermediaries for content posted on their websites, and advocate against laws that would require or encourage filtering of content. We would also encourage NTIA to work to develop and support new norms that protect the public core of the Internet. Additional details on many of the topics addressed in the notice are below.

Internet Shutdowns and Blocking

The most significant impediments to the free flow of data are efforts to block network traffic, in whole or in part. Because of our large global network, Cloudflare has significant visibility into the movement of worldwide network traffic. We have reported on countries that have restricted or revoked Internet access, including Togo, Syria, Iraq, Turkey, Libya, and Tunisia.[1] We have also seen shutdowns on Internet access in India[2], Cameroon, Chad, Ethiopia and Brazil.

In addition to shutdowns, Cloudflare often sees countries use IP blocking to prevent citizens from accessing certain content. In the fall of 2017, for example, it was widely reported that Spain raided the offices of the .cat registry and seized domains in the lead up to a referendum on Catalans' independence.[3] The Open Observatory of Network Interference (OONI) reported that at least 25 websites related to the Catalan referendum were blocked using DNS and HTTP blocking.[4]

Cloudflare has encountered this issue in countries such as Russia and Turkey, from which we receive customer complaints that visitors are unable to access their websites. Using IP blocking and other blunt tools limits free expression not only through making blocked content unavailable but also by potentially limiting access to other, unrelated, websites.

Data Localization requirements

Countries around the world have continued to pursue data localization laws that mandate that particular information or servers be stored locally. On June 12, 2018, for example, Vietnamese legislators passed a cybersecurity law requiring large technology companies to store personal data on Vietnamese citizens locally, as well as open offices in Vietnam.[5] Malaysia, Brunei and Indonesia have similar laws.

Although the stated impetus for these laws varies from law enforcement needs to protection against foreign government access to privacy, these mandates all have a similar effect of hindering global interconnection and economic development. In practice, these

[1] *See* Louis Poinsignon, The Story of Two Outages (September 7, 2017) *available at* https://blog.cloudflare.com/the-story-of-two-outages/.

[2] *See, for example,* Times of India, To Ensure Fair Exam, Rajhastan Cuts Mobile Internet Links for Two Days (July 15, 2018), *available at* https://timesofindia.indiatimes.com/india/to-ensure-fair-exam-rajasthan-cuts-mobile-internet-links-for-2-days/articleshow/64992899.cms?from=mdr.

[3] *See* Kieren McCarthy, The Register, Spanish govt slammed over bizarre Catalan .cat internet registry cop raid (September 23, 2017), *available at* https://www.theregister.co.uk/2017/09/23/spanish_government_criticized_over_catalan_internet_registry_raid/.

[4] *See* Tord Lundstrom, Evidence of Internet Censorship during Catalonia's Independence Referendum (October 3, 2017), *available at* https://ooni.torproject.org/post/internet-censorship-catalonia-independence-referendum/.

[5] *See* Mai Nguyen, Reuters, Vietnam lawmakers approve cyber law clamping down on tech firms, dissent, *available at* https://www.reuters.com/article/us-vietnam-socialmedia/vietnam-lawmakers-approve-cyber-law-clamping-down-on-tech-firms-dissent-idUSKBN1J80AE.

laws are also frequently used as a means of increasing government oversight and control, inhibiting the ability of citizens to access information and express their views.

Changes to Intermediary Liability Regimes

The last few years have seen new pressure on one of the fundamental policies that has enabled the exponential growth of the Internet -- and especially components of the Internet related to user-generated content-- over the last twenty-five years: That companies that merely move traffic over the Internet should not be responsible for the content that flows over their networks. This principle has been articulated in existing laws such as the Section 230 of the Communications Decency Act and the EU eCommerce Directive.

The European Union (EU) and several countries, for example, are currently taking steps to impose new requirements on Internet companies with respect to copyrighted material, which seek to undermine the intermediary liability protection regime. The European Commission has proposed a new Copyright Directive that would limit the ability of a wide range of Internet platforms to avail themselves of safe harbor protections like those in the U.S. Digital Millennium Copyright Act, potentially making them legally responsible for any content that their users upload.[6] In order to avoid such liability, platforms would have to turn to technological solutions such as upload filters, effectively requiring a general monitoring of the Internet.

Proposals that propose exposing companies -- particularly companies whose role in the Internet architecture is solely to transmit traffic -- to liability if they do not inspect every bit and track every customer would have a profound, negative effect on the privacy protection that users have come to expect and the freedom of expression. These types of laws also have the potential to dramatically increase the cost of providing services.□□ Sustaining laws that limit Internet instructure’s liability for content is critical to the continued growth and economic viability of the digital economy.

Restrictions on Online Content

Beyond efforts to expand intermediary liability, we have seen an increase in the number of countries attempting to explicitly restrict online content. One of the most notable aspects of these efforts is that these restrictions are increasingly coming from Western democracies.

The European Commission, for example, recently expressed an intent to pass legislation to improve the detection and removal of content that incites terrorism and

[6] *See* Caroline Greer, Copyright? Copywrong! (June 25, 2018) *available at* https://blog.cloudflare.com/copyright-copywrong/.

hatred.[7] Likewise, in 2017, Germany passed a law ('Netzwerkdurchsetzungsgesetz' or 'NetzDG') that obliges social networks to remove "manifestly unlawful" content within a defined period and at the legal assessment of the provider. Other topics include fake news,[8] content that may be harmful for minors, or content determined to be of a bullying, intimidating or humiliating nature.[9]

Although these may be well-intentioned efforts to restrict dubious content online, these types of laws restricting the availability of online content are often used to justify similar laws passed by authoritarian countries. To the extent they appear to apply not only to those who manipulate or organize content, but also to the technical providers that serve the content, they also pose serious challenges to the long-term health of the Internet, as described in more depth in the discussion of impact of restrictions on Internet infrastructure below.

Pressure on Private Industry to Restrict Content

Apart from legal restrictions on particular types of content, we have seen increased government pressure on a range of Internet platforms to undertake "voluntary" measures to restrict content perceived to be harmful, with the threat of government regulation ever present.[10] Although much of the focus of these measures falls on the largest providers, smaller companies are pressured to meet the same requirements as larger companies both directly by government entities and indirectly by larger companies. This can have a chilling effect on innovation and growth for both start-ups and SMEs which do not have the same resources readily available.

[7] *See* Note from General Secretariat of the Council to Delegation, re: European Council Meeting (28 June 2018 -- Conclusions, available at http://www.consilium.europa.eu//media/35936/28-euco-final-conclusions-en.pdf.

[8] *See* European Commission Public Consultation on Fake News and Online Disinformation, available at https://ec.europa.eu/info/consultations/public-consultation-fake-news-and-online-disinformation_en ; Rim Sarah Alouane, Macron's Fake News Solution is a Problem, *Foreign Policy* (May 29, 2018), *available at* https://foreignpolicy.com/2018/05/29/macrons-fake-news-solution-is-a-problem/.

[9] *See* Making Britain the Safest Place in the World to be Online (October 11, 2017), available at https://www.gov.uk/government/news/making-britain-the-safest-place-in-the-world-to-be-online

[10] *See, for example,* Reuters, EU piles pressure on internet giants to remove extremist content (March 1, 2018), *available at* https://www.reuters.com/article/us-eu-internet-content/eu-piles-pressure-on-internet-giants-to-remove-extremist-content-idUSKCN1GD4WW; Techdirt, At Least One Japanese ISP Gets A Jump Start On The Government's Unconstitutional Site-Blocking Plans, *available at* https://www.techdirt.com/articles/20180424/10291439704/least-one-japanese-isp-gets-jump-start-governments-unconstitutional-site-blocking-plans.shtml.

Restrictions on the use of secure technology

Another recent trend that affects both the free flow of data and free expression is country-level restrictions on the use of secure technology, like Virtual Private Networks (VPNs). Freedom House, for example, reported last year that fourteen countries had restrictions on the use of VPNs.[11] Many of these government efforts involve blocking access to the IPs offered by VPNs.

Interconnection and Cost Barriers to Internet Access

Free flow of information online is challenged when connection becomes prohibitively expensive and prevents certain people and companies from entering a market or receiving service. Countries have also restricted the free flow of information by adding taxes to access information, making access to data prohibitively expensive for potential users.

Early this month, for example, the government in Uganda imposed an excise tax on certain Over-The-Top services, including voice and messaging services and social media applications, arguing that the money was necessary to counter the effects of the gossip.[12] These efforts have largely increased the cost of access to the Internet across the board, or driven users to less secure platforms in an effort to avoid the tax.[13]

In 2016, South Korea adopted interconnection regulations designed to favor the three largest Korean ISPs and to fix the price of Internet interconnection between ISPs. This measure has led to an increase in the cost of bandwidth in Korea when almost everywhere else market pressure and new technologies are driving prices down. These regulations are hurting Internet users in Korea and causing foreign companies that offer online services and Cloud services to limit their offerings in Korea. While interconnection pricing is currently not regulated in most economies across the world, there are indications that some national regulators might emulate Korea.

NTIA can play an important role in preventing rules like those applied to international telephony interconnection in the 1980s from being resurrected and applied to today's Internet.

[11] *See* Freedom House, Freedom on the Net 2017, available at https://freedomhouse.org/report/freedom-net/freedom-net-2017.

[12] *See* David Okwii, New Tax on Over-The-Top (OTT) services in Uganda will take effect on 1st July 2018 (June 29, 2018), available at http://www.dignited.com/32755/uganda-tax-on-ott-services-effective-1st-july-2018/.

[13] *See* Quartz Africa, Lydia Namubiru, How Uganda is implementing its Controversial Social Media Tax (July 3, 2018), *available at* https://qz.com/1319826/how-ugandas-social-media-tax-works-with-whatsapp-facebook-twitter-blocked/

Impact of Restrictions on Internet Infrastructure

As an increasing number of countries attempt to regulate the content that can be accessed through the Internet, they are turning more frequently to global Internet infrastructure providers as a convenient, though problematic, choke point to effectuate these restrictions. To address the concerns raised by these efforts, Cloudflare would encourage NTIA to support the development of new international norms to protect the technical workings of the Internet and the Internet's infrastructure layer

Cloudflare's role in the Internet ecosystem is to move the bits around the globe, as quickly and securely as possible, while protecting websites from outside cyberattack. Although Cloudflare neither hosts websites nor serves content directly to users as would an Internet Service Provider, Cloudflare nonetheless is asked by foreign governments to block content numerous times per month. Cloudflare has also been asked to terminate services to particular users, even though the result of such a termination would be to open the site to cyberattack, rather than taking it offline.

Denying access to global Internet infrastructure services is a blunt tool with a profound -- and largely unseen -- effect on freedom of expression. If a website cannot be found because no registrar will provide it a domain name, no DNS provider will identify the site, or no security company will protect it from cyberattack, it is difficult to be part of the public debate in any country. Pushing Internet infrastructure companies to address problematic content -- either voluntarily or involuntarily -- also hides an authority's desire to remove content from the public eye.

Beyond direct concerns about freedom of expression, attempts to use the Internet architecture to regulate online behavior have the potential to undermine the stability of cyberspace. In order to have a functional Internet, users must trust that the technical infrastructure of the Internet will return the requested results securely and in an unaltered state.

These realities have prompted nongovernmental entities like the the Global Commission on the Security of Cyberspace (GCSC) to call for development of new norm restricting state and nonstate actors from conducting or knowingly allowing "activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet"[14] The Commission recently defined this core as including "packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of

[14] *See* Global Commission on the Security of Cyberspace (GCSC), Call to Protect the Public Core of the Internet (November 2017), *available at* https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf.

security and identity, and physical transmission media."[15] Cloudflare would encourage NTIA to support this concept.

II. Multistakeholder Approach to Internet Governance

Cloudflare appreciates NTIA's role in the multistakeholder process of Internet governance. NTIA plays a critical role in supporting efforts to improve the reliability and security of the global Internet. We would encourage NTIA to continue its engagement with multilateral organizations, with the goal of coming to consensus decisions in Internet governance that improve access, security, and performance.

Multistakeholder process

Cloudflare strongly supports the multistakeholder approach to Internet governance. Providing an environment for business, technical experts, civil society and other parties to share their ideas and air their views is a necessary predicate to solving difficult technical and policy problems and reaching consensus on decisions. This longstanding approach to Internet governance is a key reason why the Internet has continued to grow and thrive.

Recent ICANN discussions of how to address the impact of the European General Data Protection Regulation (GDPR) on WHOIS show the perils of not approaching Internet governance through an inclusive, multistakeholder approach. A week prior to the GDPR coming into effect in May of this year, ICANN proposed an interim solution for WHOIS, which, among other things, required registrars and registries to mask personal data fields and to weigh third party requests for access to non public data before responding. Rather than using the multistakeholder process to flesh out an appropriate WHOIS proposal in the years before the GDPR took effect, ICANN approved a new WHOIS Temporary Specification that many stakeholders believed to be inconsistent with the GDPR. After a number of registrars raised objections and took divergent approaches to WHOIS, ICANN filed a legal action in Germany to protect the collection of WHOIS data and to seek further clarification that ICANN may continue to require its collection.[16] ICANN's legal action thus far has been unsuccessful, although an appeal is underway.

The impact of this top-down approach, and the failure to reach consensus among affected parties, is confusion and a fragmented approach to the treatment of WHOIS. It is now incumbent upon all stakeholders to engage in the multistakeholder, bottom up policy development process that will now commence within ICANN to develop a more robust

[15] *See* GCSC, Definition of the Public Core to which the Norm Applies, *available at* https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf.

[16] *See* ICANN Files Legal Action in Germany to Preserve WHOIS Data (May 25, 2018), *available at* https://www.icann.org/news/announcement-2018-05-25-en.

solution for WHOIS, including a Unified Access Model. Cloudflare looks forward to NTIA's constructive engagement in this process.

The Internet Governance Forum (IGF) is another example of the multistakeholder model, although low levels of funding for the IGF Secretariat and delays in announcing venues and dates have affected the success of this particular forum in recent years. It should also be noted that no governance model is perfect and continuous reviews are necessary to ensure that community needs are being met. Where shortcomings are flagged, as has been the case with the IGF, improvements to the relevant forum can and should be made. Cloudflare calls on NTIA to continue to support the IGF as a viable forum for discussion on topics of interest and concern to the global Internet community, and to lend its support in any way possible.

A successful multistakeholder approach requires that all interested parties participate by sharing their thoughts and helping to develop a consensus solution. Given the global distribution of Internet stakeholders, having the participation of all relevant stakeholders has proven to be a challenge. Nonetheless, given the interconnected and transnational nature of the Internet, no other governing process is likely to be as successful.

IANA Stewardship Transition

Cloudflare has long believed that the best way to maintain a strong, stable and resilient Internet is to ensure that relevant stakeholders around the globe can provide input into how the Internet functions. The transition of the Internet Assigned Numbers Authority (IANA) to the global community of Internet stakeholders represented by ICANN helped both U.S. economic and national security interests by ensuring that the Internet remains global, scalable, and interoperable.

Cloudflare was supportive of the IANA transition and the subsequent development of the new ICANN accountability structures and mechanisms that came about as a result of the new ICANN Bylaws. By virtue of this new stewardship of the global multistakeholder community, the global DNS as we know it today is more resilient than ever and can continue to thrive. Moreover, the vibrancy of the ICANN community today, which relies for the most part on the voluntary participation of actors, is a testament to the success of the IANA transition and the model of ICANN governance.

Priorities within ICANN: DNSSEC

Cloudflare strongly supports NTIA efforts[17] to improve security for DNS by encouraging the ICANN community to review the role that third party security providers can play in easing deployment of DNSSEC. We would encourage NTIA to continue to engage with ICANN to strengthen security measures and promote DNSSEC adoption.

By adding cryptographic signatures to existing DNS records, DNSSEC allows users to verify that a requested DNS record comes from its authoritative name server and was not altered en route. This added security for DNS records helps ensure that the Internet works as intended and boosts confidence that users are receiving the sites they request.

Notwithstanding these potential benefits, widescale deployment of DNSSEC has proven to be a challenge. DNSSEC currently only works through cooperation involving registrants, registrars, third party DNS managers, and registries. Registries, registrars and third parties can generate DS keys for DNSSEC when they are the DNS provider. However, registries only receive information about the DS records directly from registrars. Thus, if using a third party DNS provider, users must log into their registrar accounts to upload third party DS records. To further complicate the issue, not all registrars support DNSSEC when the client is using a third party, effectively discriminating against third party DNS providers in the DNSSEC space. Indeed, few registrars support DNSSEC even when they are the DNS provider.

Requiring individuals to upload their own DS records from a third party, and registries' failure to support third party DNSSEC, increases friction in DNSSEC deployment. Because this process can be automated,[18] however, this friction is unnecessary. An ICANN requirement that registrars allow an automatic scan and upload of DS records -- a service that could be run by registries, registrars, or a third party operator -- would help increase the number of zones deploying DNSSEC, a result in the best interest of Internet users. Cloudflare would encourage discussion of this idea within the ICANN community and appreciates NTIA's support in this regard.

Other DNS-related initiatives to support: ANY Queries

Cloudflare would also ask NTIA to encourage the ICANN community take action on other technical initiatives to improve the security of DNS. Taking steps, for example, to

[17] *See* Letter from NTIA Adminstrator David Redl to ICANN on Registrar Issues, April 16, 2018, *available at* https://www.ntia.doc.gov/files/ntia/publications/redl_to_icann_on_registrar_issues_april_2018_1.pd.

[18] *See* Internet Engineering Task Force (IETF), Request for Comment (RFC) 7344 on Automating DNNSEC Delegation Trust Maintenance, *available at* https://datatracker.ietf.org/doc/rfc7344/?include_text=1; IETF, RFC 8078, Managing DS Records from the Parent via CDS/CDNSKEY, *available at* https://datatracker.ietf.org/doc/rfc8078/.

deprecate or shrink the size of responses to DNS ANY queries will improve DNSSEC operations and reduce the options for using DNS as a source of reflection of Distributed Denial of Service (DDoS) reflection attacks.

ANY queries are a type of operation that lists records in DNS. Instead of returning just an A, AAAA, MX, or other record, an ANY query returns all the available record types for a given name. ANY queries have few legitimate uses, but can be used for attack amplification, since these queries provide larger than necessary answers. Use of ANY queries also creates barriers to DNSSEC implementation. When responding to an ANY request, DNS services that sign queries on the fly must sign each of the various DNS records at the edge, increasing latency.

Cloudflare has been working to address the problems raised by ANY queries since 2015, first announcing that we would stop supporting ANY queries[19] and then developing a new approach of shrinking the size of the ANY query responses.[20] By deprecating ANY or reducing the size of the response to ANY queries, one more tool is removed from the arsenal of cyber attackers. We would encourage NTIA to support such efforts in engagement with ICANN, and for the ICANN community to work on this issue in pursuing the mission of ensuring a stable and secure Internet.

III. Privacy and Security

At Cloudflare, we believe that strong cybersecurity is critical to the global economy. In our interconnected world, a cyber attack on the industries of a foreign nation will have an impact on the United States. The mounting challenge of cybersecurity across the boundaries of economic sectors and national borders requires broad and deep cooperation across international borders.

Because we need transnational solutions to address cybersecurity threats, it is imperative that we find fora where government, private sector and civil society stakeholders can work together outside of times of crisis to understand each other's positions and respond to global threats. The U.S. government, and NTIA in particular, can be a leader and convener in the global debate, and to shine a light on further work that needs to be done.

[19] *See* Deprecating the DNS ANY meta-query type (March 2015), *available at* https://blog.cloudflare.com/deprecating-dns-any-meta-query-type/.

[20] *See* What Happened Next: The Deprecation of ANY, available at https://blog.cloudflare.com/what-happened-next-the-deprecation-of-any/; IETF, Proposed Standard: Providing Minimal-Sized Responses to DNS Queries that have QTYPE=ANY (March 2018).

Strong Encryption is Necessary for International Commerce and Privacy

NTIA should treat security and encryption as critical aspects of both international commerce and privacy. That means not only encouraging development and support for new encryption applications that make the Internet more secure at all layers of the Internet stack, but also discouraging global efforts to undermine encryption. Any attempt to provide “backdoors” to deal with specific anecdotes or circumstances fundamentally undermines the architecture that we need to build a secure environment. Any vulnerability that enables governments to bypass encryption efforts has the potential to be used by law enforcement and hackers alike. Intentionally compromising encryption, even for a legitimate purpose such as fighting crime, weakens everyone’s security online.

Beyond deliberate attempts to weaken encryption, some aspects of Internet transmission are not routinely encrypted, creating opportunities for abuse. At Cloudflare, we have been working to improve security at all levels of the Internet. For example, Cloudflare, in conjunction with a number of other companies, recently submitted a draft document to the Internet Engineering Task Force related to encrypting the Server Name Indication (SNI) for TLS 1.3.[21] SNI encryption could improve the privacy and security of Internet

In April, Cloudflare released 1.1.1.1, our secure recursive DNS resolver. Recursive resolvers typically send the full domain name to any intermediary on the way to the root or authoritative DNS, providing many intermediaries and outside parties easy access to a wide variety of personal browsing information. With 1.1.1.1, Cloudflare provides all defined DNS privacy mechanisms including Query Minimization and DNS over TLS.

We would encourage NTIA to support these types of technical efforts to improve security for the good of the Internet and global economy.

Harmonization of International Standards on Privacy

Because trust is central to Cloudflare’s relationship with its end users, Cloudflare has a longstanding commitment to our users’ privacy. We have publicly committed to communicating transparently, providing security, and protecting the privacy of data on our systems. To fully address privacy concerns that could undermine confidence in information networks, however, privacy must transcend particular companies or country borders. The full economic benefits of electronic commerce cannot be realized if users do not trust that their communications and transactions online are secure.

[21] *See* Encrypted Server Name Indication for TLS 1.3 (July 2, 2018), *available at* https://tools.ietf.org/html/draft-rescorla-tls-esni-00

Given these benefits, we strongly support efforts to develop technology neutral privacy frameworks that raise data protection standards. Conflicting privacy requirements, however, can create significant challenges for cross-border data flows. To facilitate data flows, we would encourage NTIA to focus on opportunities to develop and advocate adoption of data transfer mechanisms like the APEC Privacy Framework and Cross-Border Privacy Rules (CBPR).

The EU-U.S Privacy Shield has been instrumental in encouraging and facilitating transatlantic commerce and thousands of companies, Cloudflare among them, rely on this important framework in order to transfer data from the U.S to the EU. We are concerned by the recent Resolution[22] adopted by the European Parliament on the adequacy of the protection afforded by the Privacy Shield, which introduces uncertainty into this data transfer mechanism. We ask for the continued support of the NTIA for this framework, so that business can be assured of a sustainable mechanism for transatlantic data transfers.

IV. Emerging Technologies and Trends

Cloudflare appreciates NTIA's longstanding support for innovation and believes that NTIA can continue to play an important role in ensuring that the global response to new technology is thoughtful and considered.

The Internet of Things

As the Internet grows to connect not just billions of people but tens of billions of devices and sensors, it is essential that governments understand both the potential of the Internet of Things (IoT) and how to foster its growth. While much of the buzz about the Internet of Things has focused on cameras, household appliances, cars, and medical devices, many of the most important applications might very well rely on very inexpensive and simple sensors that have limited computing power and bandwidth. These simple sensors could lead to major improvements in productivity, quality, and safety on factory floors, in warehouses, in farmers' fields, and in individual homes. But this requires that these devices be protected against cyber attacks. And it requires measures to ensure that IoT devices are not infected with malware that could enable them to be used for DDoS attacks.

Some governments are considering measures to require that all IoT devices meet a long list of security requirements. In many cases, these requirements are outdated, costly, or ineffective--or all three. This kind of compliance checklist approach could make some very exciting applications of the Internet of Things too costly to be practical. Worse, it could

[22] *See* European Parliament, Motion for a Resolution to Wind Up Debate on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bMOTION%2bB8-2018-0305%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

hinder innovation by "freezing in" old technologies. The NIST cybersecurity framework represents a much better approach because it allows for innovative, new, cloud-based techniques for securing the Internet of Things without requiring that every single device online be absolutely "bullet-proof."

Future Security Initiatives

Discussions of the future of the Internet must include mechanisms to develop and implement new security mechanisms. The security of today's encryption methods, for example, is dependant on the concept that massive amounts of computing power would be required to break encryption. With the emerging possibility of quantum computing, many of today's encryption methods will no longer be secure, as the time and power needed for these computations will be dramatically decreased. Though a quantum computer is not yet a reality, we encourage NTIA to begin engaging internationally on testing and adoption of new methods for post-quantum cryptography and the need for fast deployment once a solution is found.

****

Conclusion

Cloudflare appreciates NTIA's solicitation of views on its engagement with the international community. We look forward to continuing to engage with NTIA on the topics raised in these comments.

Sincerely,

Alissa Starzak
Head of Public Policy
Cloudflare
1401 K St. NW, Suite 875
Washington, DC 20005