Access Now
www.AccessNow.org
Contact: Nathan White

May 27, 2016

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

Via Electronic Filing

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

Dear Ms. Dortch,

Thank you for the opportunity to submit comments on human rights protections for users of broadband and other telecommunications services.[1]

About Access Now

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Access Now's policy team works at the intersection of human rights and technology, furthering Access Now's mission by developing and promoting rights-respecting practices and policies. With staff placed strategically around the world, we seek to advance laws and global norms to affect long-term systemic change in the area of digital rights and online security, developing insightful, rights-based, and well-researched policy guidance to governments, corporations, and civil society. Access Now supports the work of the Federal Communications Commission (FCC) and was cited frequently in the FCC's 2015 Open Internet Order.

Access Now has particular insight into the privacy implications in the provision of internet service. In October 2014, Access Now launched AmIBeingTracked.com to enable mobile broadband users to determine wheter their service provider was using "supercookies" — special tracking headers that the carriers inject beyond the control of the user. Since its launch in October 2014, more than 330,000 people from around the world used the tool, and the results showed significant, global use of supercookies. The FCC investigated the practice, and has settled with Verizon after finding the company was failing to protect their users' proprietary information.[2]

[1] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications services, 47 Fed. Reg. 23359 (proposed Mar. 31, 2016) (to be codified at 47 C.F.R. pt. 64).
[2] Cellco P'ship d/b/a Verizon Wireless, EB Docket No. 14-17601, Order and Consent Decree, DA 16-242 (Enf. Bur. March 7, 2016) (Verizon UIDH Consent Decree).

Background

Chairman Wheeler issued a "Notice of Proposed Rulemaking" (NPRM) on April 1, 2016. The proposed rules aim to protect user privacy in the context of broadband service as Broadband Internet Access Service (BIAS) providers are the "most important and extensive conduits of consumer information and thus access to very sensitive and very personal information . . . " and there is currently no comprehensive privacy protection.[3] The proposal relies on existing frameworks, including the FCC's existing oversight of telecommunications providers and the Fair Information Practice Principles (FIPPS), around the core principles of "transparency, choice and security." Further, the proposal includes protections and definitions for certain categories of data.

- *Customer Proprietary Network Information (CPNI)* is a term previously defined statutorily in the context of telecommunications as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.[4]
- *Personally Identifiable Information (PII)* means "any information that is linked or linkable to an individual."
- *Customer Proprietary Information (CPI)* means "[CPNI] and [PII] a carrier acquires in connection to its provision of telecommunications service."

Chairman Wheeler's proposal represents a positive step toward creating rules that protect the privacy rights of consumers in the digital age. The proposal starts a crucial public dialogue about internet users' control of their data and the methods by which BIAS providers collect, process, sell, and use that data. It's an acknowledgement that regulatory intervention is needed to right the balance. In these comments, we take note of qualities of these rules:

- The emphasis of these rules is permissive. They allow Broadband Internet Access Service Providers ("BIAS Providers") to transfer data widely, only requiring opt-in for some uses.
- The rules, as proposed, would allow private data to be shared or sold to marketing companies that create detailed profiles of users.
- The rules provide few positive rights for consumers. There is no new right to access, modify, or delete this personal information, or to take that data to another provider if a user wishes to switch BIAS providers.

[3] *Supra* note 1 at 3.
[4] Communications Act, 47 U.S.C. § 222(h)(1).

- It is good that the Chairman's proposal clearly addresses data breach on a national level. The Chairman's leadership on this issue should be applauded.
- To that point, we express the need for comprehensive data protection legislation at the federal level; in the absence of such reforms, we support the FCC-FTC Consumer Protection Memorandum of Understanding[5] and more collaborative efforts to fill any gaps in transparency and accountability for privacy protection in the United States.

The Fundamental Right to Privacy

The fundamental right to privacy is recognized in international treaties endorsed by the United States, including the International Covenant on Civil and Political Rights.[6] The United Nations (UN) has applied human rights obligations to businesses in the Guiding Principles on Business and Human Rights (Guiding Principles), which asserts that governments have a duty to ensure that businesses in their territory respect human rights, including through regulation.[7] The Guiding Principles were unanimously endorsed by the UN Human Rights Council on June 16, 2011 in a resolution cosponsored by the U.S. government.[8] For their part, the OECD Guidelines for Multinational Enterprises specifically advise corporations to "take reasonable measures to ensure the security of personal data that they collect, store, process, or disseminate."[9]

Trust and certainty in the internet economy depends on widespread respect and regulatory safeguards for this human right. The FCC has increasingly worked to protect and enforce rights to privacy and freedom of expression online in recent years, and we applaud continued international leadership in this process. With the suggestions made below, we believe this framework should be adopted.

Scope

In the Notice of Proposed Rulemaking, the chairman provided definitions of key terms in order to provide guidance to both broadband providers and users regarding the scope of the privacy protections proposed. In this section Access Now offers comments about these definitions and provide answers to some of the questions posed in the NPRM.

Defining Customer

---

[5] FCC-FTC Consumer Protection Memorandum of Understanding (Nov. 2015), (https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf

[6] International Covenant on Civil and Political Rights art. 17 Dec. 16, 1966, S.Treaty Doc. No. 95-20, 6 I.L.M. 368, 999 U.N.T.S. 171 (The U.S. ratified the ICCPR in 1992.).

[7] *Ibid*. at 4.

[8] *See* U.S. Dep't of State, Bureau of Democracy, H.R., and Lab., U.S. Government Approach on Business and Human Rights (2013), http://www.humanrights.gov/wp-content/uploads/2013/06/usg-approach-on-business-and-human-rights-updatedjune2013.pdf.

[9] Org. for Econ. Dev. & Coop, Guidelines for Multinational Enterprises (2011), http://mneguidelines.oecd.org/2011ConsumerInterests.pdf.

The NPRM proposes to define customer as "1) a current or former, paying or non-paying subscriber to broadband Internet access service; and 2) an applicant for broadband Internet access service." As the NPRM recognizes, this approach would fail to extend protections to users who are not subscribers to the particular BIAS provider's service but whose data is nonetheless implicated. The FCC should take a more comprehensive view in the individuals covered by the rulemaking. Therefore, in these comments we use the term "user" instead of "customer" except where referencing the use of "customer" in the proposal

Defining Customer Proprietary Network Information (CPNI)

The NPRM references a prior definition of Customer Proprietary Network Information (CPNI), which includes, "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.[10]

An inclusive and non-comprehensive definition of CPNI is necessary to stay abreast of the changing technologies and business models in the telecom sector. We appreciate the proposal's reference to unique ID headers and the Verizon UIDH Consent Decree. This regulatory action was necessary to protect users from a threat to their privacy proven to evade detection and inserted without user knowledge or consent. It also shows that no definition of CPNI should purport or aim to be comprehensive and exhaustive, as technology changes quickly and business models continually seek new ways to monetize and market user data.

We support robust protections for all categories of information proposed in paragraph 41 in the broadband context. For example, geo-location and device identifier data is particularly in need of safeguards as more users access broadband services via mobile networks. Similarly, domain names and URLs identify the destination of web traffic and could easily reveal very sensitive and very personal information about individual users and households. Further, traffic information and the paragraph 48 categories of port, application header, application usage, and CPE information all form key points of data illuminating a larger 'fingerprint' that clearly and uniquely identifies individual users. However, we do not hold the opinion that this information be regarded as CPNI as such, but rather than it receive the strongest protection available to CPI under the new rules.

Defining Customer Proprietary Information

[10] *Supra* note 4.

Customer Proprietary Information (CPI) means "[CPNI] and [PII] a carrier acquires in connection to its provision of telecommunications service."

We support the definition of Customer Proprietary Information.

Defining Personally Identifiable Information (PII)

Personally Identifiable Information (PII) means "any information that is linked or linkable to an individual."

Companies that collect and use personal information have the responsibility and duty to respect users' right to privacy. This includes protecting information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context, no matter if this information has been provided by the user or by a third party. This reflects what the FCC defines as "linked" or "linkable" information. We therefore support the FCC proposal to define personally identifiable information as any information that is linked or linkable to an individual, taking into account that seemingly anonymous information can often - and easily - be re-associated with identified individuals.

We further support the non-exhaustive list of PII proposed in the paragraph 62 of the NPRM. This list already includes a large number of so-called metadata but could be expanded further to include this broad category of information. Metadata refers to data about the communication - such as the location, duration of a call - rather than the communications itself. BIAS Providers can collect and store metadata to track and profile users. This information can reveal a lot about a user, more than the content of the communications ever could.[11] Much of the metadata that BIAS providers collect is PII. Given the intrusive nature of metadata collection and the information it can reveal about a user, BIAS providers and the FCC must must be vigilant in assessing whether metadata is linkable to a user or users.

Metadata includes, but is not limited to:

- Location and time of a communications that it originated from;
- Information about device that sent or made the communication;
- Recipient of the communication and their location and device, and time received;
- Length of a communication or the size of a message;
- Location during social media updates, application updates or any similar automated checks on connected smartphones, etc.

Content of Customer Communications

[11] Jonathan Mayer et al., *Evaluating the privacy properties of telephone metadata*, 113/20 Proc. of the Nat'l Acad. of Sci. 5536 (May 17, 2016), http://www.pnas.org/content/113/20/5536.full

As noted above, metadata can be as revealing as content. Therefore, distinctions based solely on these broad categories are inappropriate.

However, the use or sharing, including with affiliates, of the content of user communications is a clear violation of the right to privacy, and should therefore be prohibited. Mechanisms to actively monitor communications put in place by BIAS providers have the potential to make indiscriminate surveillance easier and cheaper for anyone able to intercept those communications, thus undermining confidentiality of communication and free speech.

The failure to prohibit such measures can also have a chilling effect on the adoption and deployment of encryption technologies. Access to encryption is essential to the ability of users to exercise their rights to privacy and expression.[12] Companies willing to get competitive advantage from monitoring the content of communications - mentioned in paragraph 137 of the NPRM - could decide to throttle encrypted communications, rendering it effectively unusable.

Privacy notices

Burdens of compliance with proposed notice rules

The benefits of notice cannot be underestimated. The average user has little knowledge of how their privacy and private data are treated by broadband and internet access providers, or even who those providers and their affiliates and partners are. To begin to meaningfully exercise their rights to privacy, a fundamental right that must be better protected in the digital age, individuals require notice of where threats to their privacy lie. Accordingly, the burdens of compliance with the FCC's proposed notice rules do not outweigh their benefits of the proposed notice rules.

The FCC must ensure that BIAS providers afford all possible opportunities for notice and remedy. The costs to providers in the digital age should lower as more users take advantage of 'paperless' delivery options and electronic delivery becomes the norm. Small providers should be allowed to resort to electronic notice delivery mechanisms where reasonable to reduce costs. The cost of lost trust and damaged reputation, not to mention legal fees that can result from breach, far outweigh any notice costs to prevent such situations from occurring.

Consent

Defining "Opt-Out" and "Opt-In" Approval

We support the proposal to expand the Commission's existing definition of "opt-out" to encompass all CPI (rather than limiting it to CPNI). A 30-day waiting period is not necessary and should not be extended to broadband access; automation enables seamless instant opt-out.

[12] Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, U.N. Doc.A/HRC/29/32 (May 22, 2015).

Opt-in must be affirmative, express, and adequately informed, and must require explicit consent specific to the data and the purposes. A user must receive sufficient information to be able to understand the consequences before he or she can give their consent to the processing and use of their data. In practice, data controllers should not be able to use "pre-ticked boxes" to gain users' consent, nor imply their consent from other actions. Specific consent requires ongoing prompts, rather than a single click-wrap agreement.

To ensure user protection, consent must be freely and unambiguously given. This means, for instance, that the use of a service must not be contingent on consumer approval for the sharing of personal information with third parties or for the use of information for other purposes than the one it was originally collected.

Uses and disclosures for which no permission is necessary - 222(d) exceptions generally

We understand the need for exceptions to allow access to CPNI without customer notice or approval, in specific, targeted circumstances. However, robust and regular transparency and oversight is needed to ensure these exceptions are not abused or their scope enlarged beyond the strict letter and intent of the regulation. Further, we object to and oppose the use or disclosure of CPNI for cybersecurity purposes without specific protections for user privacy and security. Recent legislation has removed statutory protections.

Regular audits and transparency provisions must be implemented fully to ensure proper attention to these excepted uses and disclosures. The FCC should amend this rule to require providers to twice-annually report to the FCC aggregate statistics on all instances when CPNI is used or disclosed pursuant to these exceptions. This report should be made public by the FCC. In addition, the FCC should annually audit each provider's use of these exceptions, including spot checks on specific instances of such excepted use or disclosure, in order to prevent abuse of the provisions. Retroactive authorization must also be obtained.

Emergency and exigent requests routinely constitute a high percentage of the requests for user information that mobile communications providers receive from various government agencies in the United States.[13] To take one example, AT&T responded to 62,829 emergency requests in the six months from July-December 2015, as compared to 142,876 non-emergency demands from all federal, state, and local governments in both criminal and civil matters.[14] We only know

[13] *See* Am. Civil Liberties Union, *ACLU's Statement of Concerns re: H.R. 1575, the Kelsey Smith Act* (July 29, 2014) (discussing the abuse of exigent exceptions), https://www.aclu.org/aclus-statement-concerns-re-hr-1575-kelsey-smith-act.
[14] AT&T, *AT&T Transparency Report* (2016), http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html

this because of a voluntary "transparency report" that AT&T was pressured to undertake by its shareholders and civil society.[15]

Transparency reports are already expected by users and considered to be a best business practice. Reporting has been established as a norm of doing business in the information and communications technology (ICT) sector in the United States and globally.[16] The reports shed light on the scope and scale of government requests for user data, and provide crucial data on how fundamental privacy rights are treated by providers and the government.

For these reasons, we recommend the FCC require transparency reports from all broadband access providers on requests they receive from the government and other third parties for user information and content restriction; their response processes and user notification policies; compliance rates; reasons for compliance or rejection of the requests; and other categories of information to be decided in conjunction with civil society and public comment processes. Requiring reporting on these categories of information should be seen as a floor rather than a ceiling, allowing companies to continue innovating new ways to provide users and other stakeholders with essential information with regard to the privacy of their data.

Location information for emergency services

As noted above, we are wary of the exception that providers use and disclose CPNI to provide "call location information" concerning the user of a commercial mobile service for public safety. Location data is extremely sensitive and deserves the highest levels of protection. Any public safety exceptions must be strictly limited to the circumstances prescribed in 222(d)(4), and the CPNI disclosed must be the least amount necessary for the specific public safety purpose identified, and of the shortest duration and most narrow scope possible. All transparency and oversight provisions must apply and be implemented, and retroactive authorization must be obtained.

Use or disclosure of CPNI for cybersecurity purposes

Providers should not be able to use or disclose CPNI "whenever reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities" as the proposal NPRM suggests.

---

[15] *See* Press Release, Arjuna Capital, *Investors Want AT&T to Clarify Policies on Surveillance Requests: Cite Documents Charaterizing NSA Relationship as a "Partnership"* (Jan. 12, 2016), http://arjuna-capital.com/sites/default/files/ATT_Announcement_12Jan2016.pdf; Access Now, *AT&T becomes second telco to promise a transparency report* (Dec. 20, 2013), https://www.accessnow.org/att-becomes-second-telco-to-promise-a-transparency-report/

[16] Access Now, *Transparency Reporting Index* (Feb. 18, 2016) https://www.accessnow.org/transparency-reporting-index/.

Existing law, including the Cybersecurity Act of 2015, allows disclosure of CPNI "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." However, the Cybersecurity Act removed protections that limited the transfer of PII. Under the new system, users face the threat that private companies may increasingly monitor and share PII with both the private sector and the government in the name of cybersecurity. Because the statutory barriers to the sharing of private information was removed, regulatory limitations are even more important.

The proposal as written does not provide meaningful limits on sharing CPNI, which can include sensitive user information, such as location and browsing habits. Instead, the proposal should only permit the sharing of CPNI to the extent that any PII or other private data is scrubbed and only "whenever reasonably necessary to *prevent future* cyber security threats or risk of vulnerabilities."[17] Further, the language should only permit the sharing of information for cybersecurity attacks or risk of vulnerabilities only to the extent it does not risk user privacy or security.

Approval required for use and disclosure of CPI for Marketing Communications-Related Services - treatment of some or all affiliates as third parties

Privacy is a fundamental right, which must be respected online as offline. Individuals expect their service providers to protect their private information, including the "header" metadata like URLs visited, timestamps, and session data, as well as the content viewed, uploaded, and downloaded. For these reasons, we support treating all "affiliates" of BIAS providers as third parties for the purpose of requiring opt-in consent from users for any sharing with any affiliates.

To pass the *Central Hudson* test,[18] the government must *inter alia* show the government has a substantial interest in combating harms that are real, not hypothetical, and that the regulation is a reasonable fit to directly address the harm.[19] In our view, the Verizon unique ID header program shows concrete harm when providers fail to acquire opt-in consent for the sharing of private user data. In this program, Verizon shared with its advertising partners demographic identity details of Verizon users as those users surfed the web and made HTTP requests via its mobile network. In fall 2015, Verizon further enhanced its affiliations with advertisers by

[17] Letter from Ben Adida et al. Re: Cyber Threat Information Sharing Bills, to Senator Dianne Feinstein et al., (Apr. 16, 2015), https://cyberlaw.stanford.edu/files/blogs/technologists_info_sharing_bills_letter_w_exhibit.pdf

[18] In its decision in *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557 (1980), the Supreme Court articulated a four-part test to determine whether restrictions on commercial speech violate the First Amendment of the Constitution. The test requires a showing that the advertising concern lawful activity and not be misleading; the asserted governmental interest is substantial; the regulation directly advances the governmental interest asserted; and the regulation is no more extensive than is necessary to serve that interest.

[19] A subsequent case interpreting *Central Hudson* found that the government must show "real" harm that its restriction would alleviate. *Edenfield v. Fane*, 113 S.Ct. 1792 (1993).

purchasing AOL and its "online activity tracking advertising network," providing the company another vast network with which to share user data.[20] The government has a substantial interest protecting the fundamental right to privacy in the face of this type of widespread and invasive tracking. Further satisfying the *Central Hudson* test, we see that requiring opt-in is a directly effective and reasonable measure, and is not overly restrictive because it still permits sharing under user consent.

Whether the allied networks in the Verizon example above qualify as affiliates or otherwise, the complicated ties between BIAS providers and powerful advertising networks necessitate treatment of all affiliates as third parties who must obtain opt-in consent for sharing, a regulation that should withstand judicial scrutiny.

Opt-in for all other purposes

The NPRM requires broadband internet access service providers to obtain customer approval before using CPI for purposes other than marketing communications-related service; sharing customer information with affiliates providing communications-related services for purposes other than marketing those communications-related services; and sharing customer proprietary information with all other affiliates and third parties.

We support this provision. User approval for the collection and use of their data for specific and defined purposes is the prerequisite for consumer control over his or her personal information.

Historical data must not be used prior to "opt in," meaning a BIAS provider must not be able to build a profile on a consumer before approval is obtained, and then monetize that information if the user later "opts in."

To be clear, opt-out is not an appropriate mechanism to obtain user approval. Opt-out mechanisms typically suffer from cumbersome processes, offer little notice or explanation on the nature of the use, and often even deliberately obfuscate the methods and purposes of corporate programs that track users. Moreover, opt-out is useless in situations where customers have no context to understand the program or service at issue, how it impacts their privacy, or that it even exists in the first place.

The response to the Verizon header tracking example demonstrates the lack of consumer education on this issue as well as users' desire to understand the scope of collection and ability to do so when provided with the information.[21] In this case, opt-out was never sufficient, as most users do not instinctively know to look for mobile unique ID tracking headers or mechanisms to opt out; only opt-in consent based on very clear and explicit notification is appropriate.

---

[20] Nathasha Lomas, *Verizon-AOL to mind-meld ad networks to target users across apps, web and devices,* Tech Crunch (Oct. 7, 2015), http://techcrunch.com/2015/10/07/verizon-aol-ad-mind-meld-incoming

[21] Access Now, *The Rise of Mobile Tracking Headers: How Telcos Around the World Threatening your Privacy* (Aug. 2015), https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf

Use and disclosure of aggregate CPI

We welcome the FCC approach to protect the aggregated CPI. Ensuring that proprietary information is not "reasonably linkable" to a specific individual or device and prevent re-identification is rather complex. Here, it is important to make the distinction between de-identified information that is either "re-identifiable," when most identifiers are replaced by artificial placeholders, or "anonymous", where all identifiers have been stripped. Unfortunately, even "anonymous" information does not fully ensure the confidentiality of individual users. Anonymous data can also be cross-referenced with other data sources to re-identify the consumer.

BIAS providers should take all possible steps to ensure confidentiality of users. This includes anonymising information. While this technique is not perfect, it limits the retention period of this information to what is strictly necessary for a defined purposes and put data security measures in place to protect data integrity and prevent breach. However, on top of this anonymisation, providers should ensure to the greatest extent practicable that data is not reasonably linkable. All these measures provide safeguards to protect users privacy but cannot fully remove the possibility of abuses which is inherent to any data collection.

Security

The proposed two step approach articulates a general security standard and specific measures BIAS providers must take. While this approach may be appropriate in this context, the ultimate policy cannot create flexibility to excuse companies or actions from failing to provide adequate protections. All providers must be subject to minimum standards and nature and scope of the BIAS provider cannot excuse security failures. Instead, the sensitivity of the CPI should determine the protection granted. While certain information may not be highly sensitive, much is and when combined and analyzed, can provide extensive detail into individuals lives. Therefore, determining the sensitivity of a dataset should be based on a broad interpretation of potential risk.

Specific activities required of the providers under the two-step approach include risk management and employee training. While the measures on the list are appropriate, the FCC must continually update the list to ensure it keeps pace with technological advances. It is vital to avoid situations that federal legislation like Electronic Communications Privacy Act have caused, wherein changes in technology undermine the rights the laws aim to safeguard. In addition, the FCC should consider additional requirements for providers in conformity with the NIST Cybersecurity Framework. For example, access controls, authentication safeguards, and notification and patching systems are all considerations in the NIST Framework.[22]

[22] Nat'l Inst. of Standards and Tech., Framework for Improving Critical Infrastructure Cybersecurity, 23-25 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Any additional and future rules must maintain the technology neutrality that is rightly required for longevity and are implementable for service providers of any size. The rules need not specifically require the use of encryption, but instead should require providers take appropriate data security measures. To help companies respond to this requirement, the FCC may want to consider a multi-stakeholder process on how BIAS providers can encourage and facilitate widespread adoption of digital security tools and techniques, both within the industry and in the user base.

Corporate Accountability

We support the proposal to require BIAS providers to designate a senior management official to implement and maintain the provisions of the BIAS providers' data security procedures. Digital rights like privacy and freedom of expression are material issues that require board-level oversight in information and communication technology companies. We further submit that that these senior officials should report annually to the FCC aggregate information on data breaches and any misuse of user data, as well as significant updates to data security practices and protocols, and intended benchmarks defining progress on these indicators for the coming year.

Breach Notification

We agree with Chairman Wheeler's statement that "[w]e all deserve information about and control over how our data is used." To fully exercise this control, consumers must be informed in case of breach affecting their information. Data breach notification is essential to the development of strong privacy standards. It encourages data holders to properly protect data and provides users with knowledge when their data has been or is at risk of misuse. However, in order to ensure notification is effective, it should be timely, easy to understand, comprehensive, and remediation options should be clearly indicated and accessible.

Breach notification should not be limited to instances in which the breach was conducted with any particular intent, since one of the functions of breach notification is to draw attention to risks. It would also be inadvisable to add a good-faith acquisition exemption to the definition of breach. First, a requirement to determine both (a) whether good-faith existed and (b) whether data is used improperly or further disclosed are particularly difficult determinations and would create logistical challenges in enforcement. Second, employees should be properly trained and security systems should be designed to limit the risks of breach. Otherwise, the requirement that the breach be based on accessing, using, or disclosing "without authorization or exceeding authorization" would not require notification for most instances in which an employee or agent interacts with data.

The FCC should examine non-financial structures for notification, with penalties for unreasonable delay in investigating a breach. Further, there should be an easy-to-navigate system to allow individuals to issue complaints when providers fail to abide by notification

requirements. As proposed, a breach notification should be triggered based on a breach of CPI and not solely CPNI. Some of the most sensitive information that providers could store on customers falls outside the scope of the definition of CPNI, including the types of data listed in paragraph 62 of the NPRM and other data that can identify, contact, or locate persons. Whether intentional or inadvertent, data breaches have the potential to expose consumers' personal information and therefore represent a serious risk to their privacy.

Beyond notification, the FCC should examine responses to breaches that do not involve easily recognized financial harm. There are standard practices for response to breaches involving data such as credit card information or social security numbers. However, there is no standard practice for breaches that involve PII that cannot easily be tied to financial harm, such as personal photos. Stronger responses to a broader array of breaches would increase user trust in BIAS providers.

Notification to law enforcement and to Commission

The FCC proposes to require telecommunications providers to report breaches of CPI to the FCC, Secret Service, and Federal Bureau of Investigation no later than seven days after discovery of the breach.

No personal information should be included in breach notification submitted to the FCC or other governmental authorities. Personal information should only be handed over to governmental entities under a proper request made pursuant to adequate legal process. The determination to hand over personal information should not be made by the company, but instead by a judge. Once law enforcement has been notified of the breach, they may pursue a warrant to access personal information. Further, there should be no default requirement to notify police prior to notifying individuals, but the decision should be decided based on the context of the breach.

Rights to access and correct customer data

User's right to access and correct their data is essential to guaranteeing control over information. We welcome the FCC's willingness to develop a workable system that would enhance consumers' control while avoiding administrative burden for the industry.

As an element of privacy, every user should have the ability to easily access their data by simple request to their BIAS providers. The information should be provided to the consumer in electronic form or paper - based on the consumer preference - and free of charge. The providers' responses should inform the user as to which information about them has been collected and used, for which purposes, whether it has been shared with other parties and where to lodge a complaint in case of disagreement with any of these practices. Specifically, consumers should be able to seek remedy if their BIAS provider refuses to provide them with such information, unless the request is deemed frivolous by a court. Consumers should further have a right to correct their information if inaccurate or out of date.

Beyond access and correction, consumers control over their information should extend to the ability to object, to erasure, and to data portability. The ability to object enables consumers to refuse the collection and use of specific types of information. This right goes hand in hand with the European Union's recognition of the "right to erasure," which allows consumers to request that their data be purged as they end use of a service. Finally, information portability gives users the enforceable right to get a copy of their data in usable format enabling transfer to other providers. This principle prevents service lock-in and promotes competition. The FCC already recognizes the utility of "local number portability,"[23] a measure that encourages consumer choice and competition. Studies show that the high costs of switching services providers hinder competition in markets,[24] and that mobile number portability reduces wireless service prices.[25] With enhanced data portability rights, consumers would be free to move their information from one provider to another, reducing administrative burdens and barriers to competition. Interoperability between providers is an obvious prerequisite to ensure efficiency of this right. Industry should develop common standards to enable portability

Limiting collection, retention, and disposal of data

Collection of sensitive user information

We support the creation of *ex ante* rules regulating the collection of sensitive customer information and agree that the low barriers to collection have led to the vast expansion in the amount of information and collected. The authority granted in Section 222 of the Telecommunications Act to "protect the confidentiality of proprietary information" should extend to the power to enforce limitations on collection, particularly in line with the Fair Information Practices Principles (FIPPs). The FIPPs have been widely implemented within the U.S. and serve as a global model for data protection as well as the basis for state level privacy legislation. Appropriate limitations on collection in conformity with the FIPPs will serve to protect users' privacy and security while protecting trust in BIAS providers.

Retention of sensitive user information

Data retention mandates pose significant challenges to the very foundations of the rule of law and international human rights, in particular to the right to privacy. Data retention compromises data security, exposing information to government and corporate misuse, data breaches, and

[23] *See* FCC, Consumer Guide: Keeping Your Telephone Number When You Change Service Provider (Nov. 7, 2015), https://transition.fcc.gov/cgb/consumerfacts/numbport.pdf.
[24] Body of European Regulators for Elec. Commc'n, *BEREC report on best practices to faciltiate consumer switching* 8 (http://berec.europa.eu/doc/berec/bor_10_34_rev1.pdf
[25] Hal J. Singer, *The Consumer Benefits of Efficient Mobile-Number-Portability-Administration*, *s*http://www.navigant.com/~/media/WWW/Site/Insights/Economics/Consumer%20Benefits%20of%20Efficient%20MNP_Economics_030813.ashx

employee theft. It also imposes significant costs, creates liability risks and negative externalities, and wastes energy at data centers. Ultimately these costs will be passed on to users.

On data retention, the NPRM acknowledges the risk of data retention mandates for users' privacy and its impact on data security. We support this. However, BIAS operators often need to retain specific information about their consumers, for instance for billing purposes. When determining data retention limits, the essential principles of necessity, proportionality, data minimisation and purpose limitations must be respected. Data minimisation establishes that information collected and processed should not be retained or further used unless this is necessary for clearly-indicated purposes. However, the NPRM would allow for "flexible" retention periods "according to the type of relationship and use of the data." We instead recommend the FCC to adopt clear limits on data retention preventing operators from retaining customer data longer than necessary for the legitimate purpose, without any caveat or exceptions.

We further welcome the NPRM's endorsement of privacy by design regimes. We encourage the FCC to promote the development of privacy by design for companies to take a positive approach to protecting privacy, by embedding privacy-protecting principles into both technology and organizational policy. Beyond compliance, privacy should become part of the company culture, enabling companies to save in development cost and gain consumer trust.

Prohibited activities

Prohibition of use of DPI

Practices such as deep packet inspection (DPI) can have a severe impact on the right to privacy and must be carefully assessed. DPI techniques involve scanning the whole content of internet traffic. The scope of interference of these measures is increased due to the convergence of communications through the internet, including those containing sensitive personal information. [26] The impact of data monitoring techniques such as DPI have often been compared to surveillance technologies and a link between the use of deep packet inspection and internet censorship have also been established by experts.[27]

Dispute resolution

---

[26] European Data Protection Supervisor, *EDPS Comments on DG Connect's Public Consultation on Specific Aspects of Transparency, Traffic Management and Switching in an Open Internet* (Oct. 15, 2012), https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2012/12-10-15%20_Open_Internet_EN.pdf.

[27] Christopher Pasons, *Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials* (Jan. 10, 2009), http://christopher-parsons.com/Academic/WP_Deep_Packet_Inspection_Parsons_Jan_2009.pdf; Ralf Bendrath, *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection*, (Feb. 15, 2009), http://userpage.fu-berlin.de/~bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf.

The FCC should oversee the creation of a Sector-wide Process for Oversight & Transparency (SPOT) to provide users with a single point of contact at their provider to file complaints, lodge appeals, access remedy for potential violations of their privacy. Participation by users in this complaint system should not prejudice their rights to pursue remedy through other legal and regulatory fora. It would instead aim to distribute information and resolve disputes before they become situations where user trust and certainty is threatened.

The SPOT should require each BIAS provider to designate a Privacy Office to handle complaints, in a regulated, predictable, and rights-respecting process that comports with principles for operational-level grievance mechanisms.[28] Such mechanisms, so long as they do not supplant or prejudice more formal forums for remedy, can help resolve conflicts efficiently and prevent escalation in some cases.[29] The FCC can convene the Privacy Offices to share best practices and receive training.

Each Privacy Office participating in the BIAS SPOT should issue an annual report to the Chairperson of the FCC, who should then issue a report aggregating results of the complaints process with recommendations to improve overall efficiency and effectiveness.

Conclusion

Given the breadth and reach of the United States digital economy, the rules put forward by the FCC have the potential to influence standards globally. Such impact requires careful consideration and provide the U.S. with a unique opportunity to lead the development of comprehensive user-centric protections on the Privacy of Customers of Broadband and Other Telecommunications Services. We support the FCC's actions to put consumers in control of their information and protect their right to privacy. We encourage the FCC to continue to move forward with this rule making and encourage the Commission to include specific recommendations in this document.

***

Access Now (www.accessnow.org) is a 501(c)(3) non-profit organization that defends and extends the digital rights of users at risk around the world.

---

[28] For example, Guiding Principle 31 of the UN Guiding Principles on Business & Human Rights recommends that operational-level grievance mechanisms be legitimate, accessible, predictable, equitable, transparent, rights-compatible, and a source of continuous learning. *See* Guiding Principles on Business and Human Rights: Implementing the Protect, Respect, and Remedy Framework, U.N. Doc. HR/PUB/11/04 (2011).

[29] Caroline Rees, *Grievance Mechanisms for Business and Human Rights: Strengths, Weaknesses and Gaps* (Jan. 2008), https://www.hks.harvard.edu/m-rcbg/CSRI/publications/workingpaper_40_Strengths_Weaknesses_Gaps.pdf .