Attachment – Additional Questions for the Record

The Honorable Greg Walden

1. How and why does the FCC's approach fall short to protect consumers in current form? Do you have any suggestions for the FCC on how it could improve the proposal?

   The Federal Communications Commission ("FCC") approach does not adequately protect consumers because it would create a bi-furcated regime for protecting privacy between the FCC's rules for Internet Service Providers ("ISPs") and the Federal Trade Commission's ("FTC") enforcement framework for the rest of the internet ecosystem. A holistic approach to internet privacy would provide the type of certainty and consistency that consumers expect, and would ensure that all entities that collect, use, and share information about consumers' online activities would respect consumer privacy in the same manner.

   The FCC could improve its proposal by learning from the FTC's privacy experience and listening to the concerns raised in the FTC's Comment to the FCC. The FTC's comments support a privacy framework focused on consistency across industries and on the sensitivity of consumer information.

   Instead of protecting consumers, the FCC proposal could harm them by making it more difficult for ISPs to provide services and capabilities their customers want. Most broadband consumers have shown – by their behavior under the FTC framework – that they are comfortable with having non-sensitive data utilized to provide them with customized advertising and offerings. Those that prefer not to have their data used in such a manner have ample opportunity to opt-out.

   By requiring opt-in approval, the FCC's approach could harm consumer welfare by needlessly restricting data uses preferred by most consumers. While the FCC proposal makes it harder for ISPs to offer services and capabilities their customers favor, it fails to materially improve the privacy of consumers, because every non-ISP internet company would continue to be subject to different restrictions on their use of broadband data. Consumers would be made worse off by a framework that makes it more difficult for them to receive information about offerings and capabilities they enjoy today, while failing to provide any meaningful improvement in privacy protection.

2. During your tenure at the FTC, first as a commissioner, then as chairman, did the agency ever come to the conclusion that ISPs alone posed a unique problem in terms of privacy that warranted a more stringent and restrictive set of privacy obligations for them? Has anything changed since then?

   a. During your tenure as FTC Chairman, the White House and Commerce Department also issued a privacy report and Consumer Privacy Bill of Rights regarding commercial uses of data. Did the Administration single out ISPs for special treatment or identify any unique problems associated with ISPs in setting forth its privacy policies and standards? Has anything changed since then?

The FTC's 2012 Privacy Report did not single out ISPs as posing unique privacy challenges; rather, the Report concluded that "to the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns."[1] The FTC also concluded that "any privacy framework should be technology neutral."[2] Thus, the FTC report did raise potential concerns about "large platform providers," but not just ISPs. In the wake of that Report, the FTC gathered further information in a workshop and carefully examined the question of whether large platform providers, including major search engines and browser providers, as well as ISPs, should be subject to heightened restrictions and ultimately refrained from doing so.

Similarly, the Administration concluded that "[i]t is important that a baseline [privacy] statute provide a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions."[3]

The Honorable Adam Kinzinger

1. Mr. Leibowitz, in your testimony you went into detail on the differences between the FTC's current approach to data breach notification and the FCC's proposed regulation. You say that a balanced approach will avoid over-notification which would confuse customers and cause them to ignore notices they receive. Can you elaborate on this point? How does an optimal approach determine when a customer needs to be notified?

   A balanced approach would limit the type of information for which an ISP would be required to notify consumers in the event of a breach of sensitive information the disclosure of which could result in identity theft or other financial harm. Unfortunately, the FCC's extremely broad proposed definition of "customer proprietary information" would require breach notification even for information the disclosure of which does not present a risk of harm to consumers. Consumers want to (and need to) be notified about breaches that present the reasonable risk of harm. But when consumers receive notices about breaches related to mundane, non-sensitive information, they will stop paying attention to breach notifications. Thus, when the notices are truly important, consumers may miss the opportunity to protect themselves.

2. Mr. Leibowitz, the FTC staff noted that the FCC's proposed data breach notification timeline would not allow companies adequate time to conduct an investigation. Do you agree with that conclusion?

---

[1] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 14 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-tradecommission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[2] *Id. at 56.*
[3] Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 36, January 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

10 days is not enough time to conduct an investigation. In 10 days, a company may not be able to determine whether a breach was inadvertent or whether it could result in identity theft or other financial harm. It is critical that companies have enough time to take remedial steps to address a breach and to conduct a comprehensive investigation before notifying consumers. The FTC expressed concerns about the FCC's proposed breach notification timeline, which is considerably shorter than each of the 47 state data breach notification laws.

The Honorable Gus Bilirakis

1. Mr. Leibowitz, Professor Lawrence Tribe from Harvard had an interesting Constitutional argument in his comments to the FCC about restrictions to commercial speech. Do you think we are looking at another issue in which we will all become court watchers and have to wait for months for a First Amendment challenge to work its way through the courts?

   The FCC's proposed requirements would impose a substantial burden on speech because they would preclude ISPs from engaging in important and relatively routine communications with their customers. Such requirements would prevent the type of targeted speech from which consumers benefit, and would prevent speech which will continue to be permitted for non-ISPs. In order to pass constitutional muster, such a burden on commercial speech must satisfy each element of the three-part test set out in *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557 (1980), which asks whether (1) "the government interest is substantial"; (2) "the regulation directly advances the governmental interest asserted"; and (3) "it is not more extensive than necessary to serve that interest."

   Professor Tribe concludes that the NPRM fails on each prong of the *Central Hudson* test.[4] First, in Professor Tribe's view, the government has not articulated a substantial interest in restricting ISPs' ability to use customer information already in its possession, particularly where that information is not disclosed to third parties. Second, as discussed above, the NPRM completely ignores the fact that, even if the proposed highly burdensome rules are imposed on ISPs, edge providers will continue to collect and share precisely the same type of consumer information. For this reason, Professor Tribe has concluded that this asymmetry demonstrates that the NPRM cannot be considered to directly advance an important governmental interest. And third, Professor Tribe believes that the NPRM's proposed opt-in rule is not narrowly tailored because a less obtrusive opt-out rule would serve any legitimate government interest in protecting consumers from first-party marketing.

   The FCC is already familiar with the *Central Hudson* constraints on the restrictions the agency may impose pursuant to Section 222 of the Communications Act (47 U.S.C. § 222). In *U.S. West Communications, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), the

[4] Laurence Tribe and Jonathan Massey, The Federal Communication Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment, at 4 (May 27, 2016), http://www.ctia.org/docs/defaultsource/defaultdocument-library/ctia-ncta-ust-file-tribe-paper.pdf.

U.S. Court of Appeals for the 10th Circuit struck down the FCC's attempt at regulations governing Customer Proprietary Network Information ("CPNI") with respect to voice communications. In that case, the court determined that the collection and sharing of CPNI among affiliates constituted speech and that the FCC's opt-in regime did not satisfy intermediate First Amendment scrutiny. As Professor Tribe notes, the proposals in the NPRM "represent a *much larger* burden on speech and are far *less* tailored to any substantial governmental interest" (emphasis in original).[5] Because the NPRM's proposed opt-in requirement poses a substantial burden on speech and is not tailored to any substantial governmental interest, it is susceptible to a constitutional challenge.

2. Mr. Leibowitz, can you expand on your concern that this new framework creates a serious risk of unforeseen consequences? Do you think the FCC appropriately took these into account? In your time at the FTC, how did you evaluate similar potential disruptions to consumer expectations and unequal application of consumer protections?

   The FCC's proposal would substantially limit an ISP's ability to market its own products and services that are not "communications-related" to its own customers, including home security, energy management, and music streaming. That means consumers may not know about innovative or lower-priced offerings from which they would benefit. The FCC's NPRM does not provide an economic analysis, and its proposal does not appear to take these adverse consequences into account.

   During my tenure at the FTC, we attempted to ensure that consumers had the opportunity to make informed choices about services and products, and that they knew about a breadth of alternatives. If a company failed to adequately inform consumers about the consequences of a product or service – or worse, deceived consumers – we would take action against that company. But ultimately, we believed in the ability of consumers to make choices themselves, and we believed that allowing such choices drives innovation, competition, and lower prices. That thinking seems absent in the "command and control" approach of the NPRM; as a result, it is more likely to harm than benefit the very consumers the FCC is supposed to serve.

   The massive and unprecedented breadth of data covered by the FCC proposal threatens to harm consumers – and, potentially, basic Internet functionality and practices employed today – in ways known and unknown. It is not just ISPs that are saying this. The Internet Commerce Coalition, which includes edge providers, notes that the FCC proposal "covers a broad swath of information that is not in the least sensitive" and sweeps in "information that travels widely across the Internet whenever a user communicates." Parties with IT, network engineering, and security expertise express particular concern with regard to the FCC's proposal to restrict the use of IP addresses, device identifiers, domain information, and other data elements which cannot, on their own, identify specific persons, but which are basic elements of network engineering and operations. The FCC needs to take more time to fully examine a raft of complex technical issues that could have serious consequences for consumers' Internet experience.

---

[5] *Id.*