
4 Monroe Parkway
Suite K
Lake Oswego, OR 97035

May 16, 2017

The Honorable Jennifer Williamson
Oregon House of Representatives House Majority Leader
Chair, House Committee on Rules, Oregon State Legislature
900 Court St. NE, H-295
Salem, Oregon 97301

Leader Williamson and Members of the Committee:

Thank you for your invitation to testify regarding broadband and Internet privacy. I am the founder and executive director of the World Privacy Forum, a 501(c)(3) non-partisan public interest research group based in California and Oregon. We focus on conducting in-depth research on emerging and contemporary privacy issues as well as consumer education.

My involvement in these debates, and that of the World Privacy Forum's, is longstanding. I have worked in the area of privacy for more than 20 years, beginning with my work as a principle investigator and privacy and security researcher at the Denver University School of Law's Privacy Foundation. I have testified before Congress, including the US Senate Judiciary Committee, as well as many federal agencies; my publications include numerous books, research, reports, articles, and regulatory comments, including a reference book of relevance for today's topic, *Online Privacy* (ABC-CLIO). I have also done a great deal of work internationally, both as a member of the TransAtlantic Consumer Dialogue, at the OECD, where I am an advisor on privacy and data, and most recently, this April, as a participant in the G20 Digital Ministerial.

Regarding the issue at hand today, the combined lack of broadband privacy protections for consumers at the federal level -- which include the lack of Congressional legislation, and the lack of protections from the FCC and the FTC -- work together to create a substantial gap in consumer broadband privacy protection. State action is reasonable, and in fact necessary.

The World Privacy Forum believes that federal legislation codifying strong, pro-consumer broadband internet service providers privacy requirements would be the preferred outcome to give both consumers confidence that consumer data would be protected and innovators clarity through bright line rules outlining their data responsibilities. Absent this, state level legislation mandating strong protections for Oregon's citizens is the best choice. In either case, federal regulatory efforts at the agency level – due in no small part to the fact that election outcomes periodically change leadership control over key regulatory bodies such as the FCC and the FTC -- have to date been inadequate to ensure consistent, meaningful broadband privacy protections for consumers. Further, recent events leave regulatory jurisdictional questions unanswered, consumers' private data potentially exposed, and innovators without clarity.

The reason I am here in person today is to further discuss these issues, both because of my experience and expertise in privacy, and also because I am a resident of Oregon, thus giving me double interest in the outcome of this hearing.

I would like to discuss three points with you today.

**I. The U.S. Federal Trade Commission cannot adequately enforce consumer broadband privacy, leaving a substantial gap in consumer protections**

As is well-known to the Committee at this point, the Federal Communications Commission (FCC) put broadband and Internet Service Provider (ISP) rules in place, set to go into effect this spring. However, the broadband privacy rules were rolled back by the U.S. Congress in such a way that they never went into effect due to the use of procedures pursuant to the Congressional Review Act (CRA). Revocation by use of the CRA not only eliminates the privacy rules set forth by the FCC in October 2016, it further limits the ability of the FCC to craft substantially similar regulatory protections.

Since the FCC broadband privacy rules have been repealed, much discussion has ensued regarding the U.S. Federal Trade Commission (FTC) and whether it is the preferable agency to enforce consumer broadband privacy. The World Privacy Forum regrettably concludes that the FTC lacks the legal authority to fully protect consumer broadband privacy, for reasons I explain below.

First, apart from questions regarding the legal underpinnings for the FCC's jurisdictional claims pursuant to Title II of the Telecommunications Act of 1996, the FTC does not have rulemaking authority akin to the FCC's. As numerous regulatory power authorities have concluded,[1] under Magnuson-Moss, the FTC's rulemaking authority is severely

[1] For a discussion of FTC rulemaking authority, how it was developed, and how it operates, *see*: Timothy Edward Deal, *Moving Beyond 'Reasonable': Clarifying the FTC's Use of Its Unfairness Authority in Data Security Enforcement Actions* (February 4, 2016). Fordham Law Review, Vol. 84, No. 5, 2016. Available at SSRN: https://ssrn.com/abstract=2727818. *See also* comments of FTC Chairman Edith Ramirez re: the time-consuming nature of Magnuson-Moss rulemaking procedures, and how that impacts its viability as a consumer protection mechanism: *Prepared Statement of the Federal Trade Commission on Data Security*: Before the Subcommittee on

constrained under Section 18 of the FTC Act to a partly-adjudicated process which is time consuming, complex, and for most purposes, not a genuine option for consumer protection due to the extremely high barriers it creates.[2] The likelihood of Magnuson-Moss being repealed at this time is very nearly zero.

Second, the FTC does not have sure footing regarding oversight over Title II activities. At present, the FTC's jurisdiction to regulate the consumer data privacy actions of broadband providers remains in doubt as many perceive a regulatory void that the FTC's current authority does not fill. As FTC Commissioner Terrell McSweeney commented on Wednesday, May 10: "The regulatory gap will not be closed until Congress repeals the common carrier exemption in the FTC Act."[3] This will be true even if the 9th Circuit, after its *en banc* rehearing of *FTC v. AT&T*, decides to reverse its earlier decision. Thus the barriers that exist for the FTC to act as a robust, proactive protector of consumer broadband privacy are significant, and it will take much effort at the national level to put those protections in place. It is not reasonable to expect that the U.S. Congress will act to both repeal Magnuson-Moss and pass new legislation affording the FTC jurisdiction over Title II and full broadband business and privacy activities.

## II. Privacy regulatory rules for broadband and ISPs are good for business

For the digital ecosystem to flourish, there must be consumer trust in that ecosystem. Unfortunately, consumer trust in the online environment has been shattered by the rollback of the FCC broadband privacy rules. For example, a May 2017 survey by Bloomberg BNA revealed that 95 percent of consumers are uneasy about privacy after the FCC privacy rule repeal.[4] Consumers do not trust the companies that provide the backbone of the digital ecosystem right now to not misuse their personal data, and that is not good for ISPs, broadband providers, nor for the other participants in the digital ecosystem.

At the G20 Digital Ministerial this April, the focus of the delegates was on the issue of trust in the digital ecosystem, and how important that trust is for business and consumers. I was particularly impressed by the testimony of one participant, representing Telefonica on a panel focused on consumer trust, who repeatedly and emphatically stated: "Data is

---

Commerce, Mfg. & Trade of the House Committee on Energy & Commerce, 112th Cong. 11 (June 15, 2011). Available at: https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf. See p. 11 in particular.

[2] FTC Administrative Staff Manual, Rulemaking, Chapter 7, U.S. Federal Trade Commission. Available at: https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf.

[3] FTC Commissioner Terrell McSweeney as quoted in: Angelique Carson, *Ninth Circuit to Hear FTC v. At&T en Banc*, IAPP, May 10, 2017. Available at: https://iapp.org/news/a/ninth-circuit-to-hear-ftc-v-att-appeal-en-banc/.

[4] Alexis Kramer, *Americans Uneasy About Data Privacy After FCC Rule Repeal Survey Says*. BNA, May 10, 2017. Available at: https://www.bna.com/americans-uneasy-data-b73014450726/.

*not* the new oil."[5] Although I do not have first-hand knowledge of Telefonica's internal data activities, the company is by all appearances working to overcome the perception that customer data is a commodity for the company, and their statement was welcome.

One of the most important ways for business to earn consumer privacy trust is to provide consumers with essential privacy rights, including transparency and meaningful choices regarding data uses. There is no need to re-invent this wheel and somehow figure out what the core privacy rights might be -- fundamental Fair Information Practices are already well-established. FIPs came into being in the U.S., and are now a global agreed-upon set of principles that form the backbone of almost all U.S. federal privacy law,[6] including the Privacy Act of 1974, HIPAA, the Fair Credit Reporting Act of 1974 (FCRA), and other legislation. The FIPs principles include transparency, accountability, the ability of consumers to access and correct information, among other principles.

The credit bureaus have had to comply with, for example, the Fair Credit Reporting Act for many decades now; thus preventing numerous consumer harms. I for one do not wish to imagine a world in which I could not see my credit score, correct errors in my credit bureau report, recover fully from negative changes to my credit record due to the activities of an identity thief, and more. Commonsense, pro-consumer regulations guiding the credit industry provide a useful model for the ideal broadband regulatory structure. Commonsense privacy rules will not hamper broadband providers but will re- instill consumer confidence that they may use broadband services without fear that their privacy will be compromised or their data monetized and used in ways to which they would not consent. We will look back at the time that broadband providers were not required by statute to provide even the most basic privacy protections for consumers, and wonder why it took us so long to provide fundamental, reasonable, basic protections for people regarding their Internet activities, which are every bit as essential as credit activities in today's world.

In the long term, good "rules of the road" help business. Rules provide accountability, which is essential, and if the rules are crafted properly, with public support, they can also serve as a key mechanism to foster consumer trust.

## III. Privacy rules for broadband and ISPs are good for consumers

Broadband privacy rules can reduce harms to consumers that come from non-transparent information use and sharing, including uses and sharing of ISP data. Currently, due to the FCC broadband privacy rule repeal, consumers are bereft of clear rules that broadband providers must follow to protect consumer data and give consumers meaningful choice

---

[5] Comments of Carlos Lopez Blanco, G20, *Multi-Stakeholder Conference Digitalization: Policies for a Digital Future*, Panel 3: *Encouraging Transparency -- Creating Confidence in the Digital World*. Dusseldorf, April 6, 2017.

[6] Robert Gellman, *A Basic History of Fair Information Practices*. Available at: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020.

regarding the sharing or sale of some of their data. Only those people residing in a state or a city that has enacted meaningful consumer broadband privacy rules will now have specific, enforceable external rules for broadband providers.

Data protections are important because modern data uses are complex, and these uses are not nearly transparent enough most of the time. I have, for example, testified before Congress multiple times on the activities of "data brokers,"[7] companies which specialize in collecting, analyzing, and selling personally identifiable information (or data sets) to third parties. This activity most often takes place without consumer notification or explicit consent. This is true for data relating to health, age, spending habits, and much more.

Unbounded data sharing and sale can potentially be damaging to consumers and may have meaningful marketplace impacts. In our report, *The Scoring of America*,[8] my co-author and I wrote about how companies and other entities use consumer data to analyze consumers, create categories of consumers, and to give customers scores. For example, "churn" scores are a well-known scoring type that predicts customer loyalty; these scores are often used by cable and broadband companies.[9] Not all scores are negative, and scoring by itself is not always an activity with deleterious consequences. However, a number of issues do exist, for example, unregulated scores are seldom made readily available to consumers.

Discussion about consumer data and its many uses is of particular relevance to cable companies, telecommunications companies, ISPs, and broadband providers for several reasons. First, broadband providers provide an essential service. It is no longer reasonable to think that a person can simply or easily just opt out of having Internet access. Second, because of the nature of their services, ISPs have access to a wealth of incredibly detailed consumer data, including potentially web browsing and other data such as geolocation. These data sets are highly analyzable and have superior informational value. Some ISPs do not sell or share data, some do. Practices vary.

There is a data practice worth mentioning called "data appending," which is common to many businesses.[10] Data append is when a company purchases additional data about their customers from data brokers and/or data aggregators to add to their pre-existing customer

---

[7] See *Data Brokers: Is Consumers' Information Secure?* Testimony of Pam Dixon before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law, Nov. 3, 2015. Available at: https://www.judiciary.senate.gov/meetings/data-brokers_is-consumers-information-secure.

[8] Pam Dixon and Robert Gellman, *The Scoring of America*, World Privacy Forum. April 2014. Available at: https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

[9] *Supra* note 8 p. 51.

[10] For a list of data append service providers, *See:* Direct Marketing Association Vendor Search, Data Append. May 10, 2017. Available at: http://dataandmarketingsearch.com/Guide/SearchListing?searchTerm=data+append&PageNo=1&PageSize=10&sectionType=&categoryId=0&headingId=0&Region=&rbPhraseType=2&StateProvince=&CityOrZip=.

data. This appended data is typically described as "demographic" or "purchase history" data, and can include a myriad of information -- like number of children, educational attainment, rent/own home, exact income, and numerous additional categories of information.[11] Any ISP or broadband provider that engages in data append practices can create an extraordinarily rich profile of an individual. Again, practices vary. Will Oregon broadband customers have the right to know about *and opt out of* data append practices? Right now, data append will be up to the company's discretion. I looked up my Oregon broadband provider's relevant privacy policy, and found the following language, which is regarding data append practices; the relevant language is in bold:

> *What kind of information does Comcast collect and use to improve your cable services and deliver relevant advertising?*
>
> *Comcast's cable system, set-top boxes, and other equipment generate activity data that we collect and store. We use this information for a number of purposes including to determine which programs are most popular, how many people watch a program to its conclusion, and whether people are watching commercials. As described below under "How does Comcast use personally identifiable information and CPNI?," we may also provide information like subscriber lists or certain de-identified, anonymous, and/or aggregate information (such as activity data) to third parties working on our behalf -- such as audience measurement or market research firms.* ***We, or these firms, working as our service providers, may combine this information with aggregated or non-aggregated demographic information (such as census records) and other audience attributes, such as purchasing data, demonstrated interests (for example, in sports programs or movies), loyalty programs, organizational affiliations, advertiser customer lists, and the like to provide us with audience analysis data.*** *We require third parties working on our behalf to treat all information we provide as confidential and to use it only for Comcast's business purposes. We may also work with academic or research interest groups to analyze de-identified, anonymous, and/or aggregate information we provide to them for specific purposes or projects.*[12]

A general issue I note here is regarding the use of *aggregate* and *non-aggregate* customer data. The term *aggregate data* is often misunderstood in the context of consumer data use discussions. Too often, there is an idea that aggregate data is not identifiable data, and is "anonymous." The re-identification of supposedly "de-identified" aggregate customer data is a known issue of concern today. Modern research has repeatedly demonstrated that it only takes a modicum of identifiers to re-identify individuals in datasets that were

[11] For a more complete roster of data that can be sold about consumers, please see *Scoring of America*, *Supra* note 8, pages 30-38.

[12] Comcast Customer Privacy Notice For Cable Video, High-Speed Internet, Phone, and Home Security Services, Comcast, May 11, 2017. Available at: https://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html?pc=1.

previously "anonymous."[13] The body of research is now so compelling and unambiguous that I no longer use the term anonymous to describe de-identified data sets anymore, as anonymity is not a guarantee when discussing aggregate data sets. Data scientists from Cornell have recently published research that shows aggregate mobile data, including from apps, can be re-identified, in some cases with up to 98 percent accuracy.[14] I note that the city of Seattle included language about aggregate data sets and de-identification in its recent *Seattle IT Rule 2017-01*[15] regarding broadband privacy. The language is in bold in the following section:

> *"Cable Operators shall submit a letter to the Director of the Office of Cable Communications self-reporting their compliance with Section 21.60.825 of the Cable Code by September 30, 2017 and annually thereafter. At a minimum, this letter shall contain the following:*
>
> - *The process by which customers may opt-in to sharing or other use of web browsing activity, other internet usage history, and use of their personally identifiable information.*
> - ***Whether customer web browsing activity or other internet usage history is shared in a detailed or an aggregated manner***
> - ***Deidentification techniques used to protect individual customer privacy before web browsing activity or other internet usage history is shared***
> - *Process by which customers may appeal perceived privacy harms from this data sharing process,"...*[16] *[bold added.]*

As you can see from even this brief discussion about consumer data uses, data uses today are extremely complex, and consumers have few opportunities to assert rights in regards to these data uses, including data append practices on "non-aggregate" or personally identifiable data. Meaningful rights are available in laws regarding credit reporting data, health data, video rental data, and other data types, but not yet the very rich data set of Internet data usage. It would be of significant benefit to consumers to create rules regarding a very important data set, that of their Internet data uses.

## IV. Conclusion

As discussed, fundamental gaps in consumer broadband privacy now exist, concomitant with growing consumer distrust of the digital ecosystems and of the companies providing broadband and Internet access. Consumers are right to want broadband privacy

---

[13] See in general the work of LaTanya Sweeney, Harvard. See also: LaTanya Sweeney, Only You, Your Doctor, and Many Others Know, Harvard Journal of Technology Science, 9-29-2015. Available at: https://techscience.org/a/2015092903/.

[14] Fengli Xu et al., Trajectory Recovery from Ash: User Privacy is NOT Preserved in Aggregate Mobility Data, V.2., WWW 2017, accessed via ArXiv:Cornell University Library. Available at: https://arxiv.org/abs/1702.06270.

[15] *Seattle IT Rule 2017-01*, Pursuant to SMC 21.60.825(k),City of Seattle, May 3, 2017. Available at: http://www.seattle.gov/Documents/Departments/SeattleIT/SeattleRule_ITD-2017-01.pdf.

[16] *Supra,* note 13.

protections -- we are well into the digital era, and more and more people know how important their data privacy is to their current and future well-being. Consumers are not demanding unreasonable concessions, just fair treatment and a modicum of control over the digital aspects of their lives. This is reasonable.

As state lawmakers, you have the opportunity to address the lack of protections for consumers' broadband data and assist business and consumers by putting broadband privacy rules in place. This is an important moment in history. I remember well the identity theft debates of the 1990s, where financial sector businesses were reluctant for states to pass rules that would help people have the tools they needed to recover from identity theft. Fortunately, the states recognized the great harms of identity theft, and slowly but surely, consumers gained the protections they needed.

Similarly, consumers need broadband privacy protections to have the rights and tools they need to have choices about how their geo-location history, detailed web browsing history, and other identifiable data flows arising from their Internet-based activities are used.

This is a complex topic, and I have been brief. I am pleased to answer any questions you may have, or assist with more detail on topics I have touched on here.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum