Testimony of

Hance Haney
Director and Senior Fellow
Technology & Democracy Project
Discovery Institute

Before the

Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

On

Protecting Customer Proprietary Network Information in the Internet Age

July 11, 2018

Dear Chairman Blackburn, Ranking Member Doyle and Members of the Subcommittee,

Section 222 of the Communications Act of 1934, as amended, governs the privacy practices of telecommunications common carriers, including local, long distance, commercial mobile wireless service (CMRS) and interconnected voice-over-Internet Protocol (VoIP) providers, such as AT&T, Sprint, and Verizon. Among other things, carriers are generally prohibited from using, disclosing or permitting access to individually identifiable customer proprietary network information (CPNI) without customer approval.[1]

CPNI is defined as: 1) information relating to the "quantity, technical configuration, type destination, and amount of use" of a telecommunications service received by a particular customer and 2) information pertaining to telephone exchange and telephone toll service contained in the

[1] 47 U.S.C. §222(c)(1).

billing that a customer receives.[2] CPNI includes, with some exceptions, "virtually all information about a customer's use of network services" that a telecommunications carrier may acquire from providing those services.[3] Examples of CPNI include detailed descriptions of voice calling history (including the time, location and duration of the call, as well as the telephone numbers from and to which the call was placed),[4] and the products and services purchased or subscribed to by an individual customer—such as call waiting, caller I.D. and call forwarding.[5] There are exceptions to the rule.

Among the exceptions, telecommunications carriers are permitted to use, disclose or permit access to CPNI *without* customer approval in the course of marketing service offerings to their current customers, provided those services are within the carrier's own "category" of service.[6] The service categories are: local, long distance and wireless. Thus, telecommunications carriers may not use any CPNI in their possession to market to a prior customer who switched to another carrier, or market to customers who are receiving another category of service from another provider. Otherwise, in order to use, disclose or permit access to CPNI for the purpose of competing in the marketplace, carriers have to obtain "opt-in" approval (*i.e.*, the carrier must obtain affirmative, express consent in advance from the customer). Carriers may obtain approval through written, oral or electronic methods, but they bear the burden of demonstrating that oral approval has been given in compliance with FCC rules, and they must maintain records of approval—whether oral, written or electronic—for at least one year.[7]

---

[2] *Id.*, at §222(h)(1).
[3] Peter W. Huber, *et al.* Federal Telecommunications Law (2d. Ed.) (Aspen Law & Business, 1999) at 438.
[4] 47 C.F.R. §64.2003(d).
[5] *Id.*, at §64.2005(c)(3).
[6] *Id.*, at §64.2005(a).
[7] *Id.*, at §64.2007(a).

Broadband

Section 222 does not apply to broadband services, which are classified as an "information" service.[8] Therefore, even though broadband services could be thought of as being provided by telecommunications carriers, the statute and the regulations look to the service provided, not to the provider of the service. Accordingly, broadband is excluded from the ambit of Title II of the Act—including Section 222 and the FCC's CPNI rules. Instead, broadband is subject to the unfair and deceptive acts and practices authority of the Federal Trade Commission (FTC). This is the same authority that governs video streaming services like Netflix and YouTube, search engines like Google and Bing, social networking sites like Facebook and LinkedIn, e-commerce sites like Amazon and eBay and user-generated media sites like Twitter and Pinterest (*i.e.*, the entire Internet ecosystem). In other words, none of the services I have referenced here fit within the statutory definition of CPNI.

The FCC concluded in 2015 when it briefly classified broadband as a "telecommunications" service that the CPNI rules, which were designed to address concerns relating to voice service, were not well suited to broadband Internet access service.[9] The CPNI rules—as they were then and are now—do not address "many of the types of sensitive information to which a provider of broadband Internet access service is likely to have access," according to the Commission, "such as (to cite just one example) customers' web browsing history."[10] A leading industry participant expressed the opinion that it was "unclear what these privacy protections would even mean in the broadband context…"[11]

---

[8] *Restoring Internet Freedom*, WC Docket N. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2018) (*Internet Freedom Order*).
[9] *Protecting and Promoting the Open Internet*, WC Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5823-24 , para. 467 (2015) (*Title II Order*).
[10] *Id.*
[11] Verizon *Ex Parte* Letter at 7-8, GN Docket No. 14-28 (Jan. 26, 2015).

The *Privacy Order* adopted by the FCC in October 2016 modified the CPNI rules to account for the unique aspects of broadband service offerings, which were classified as a telecommunications service at the time.[12] The *Privacy Order* created a stricter privacy framework for broadband service providers than for other participants in the Internet ecosystem—creating asymmetric regulation that could inhibit competition and jeopardize private investment in broadband networks. Specifically, carriers were required to obtain opt-in consent in order to use, disclose or permit access to virtually all information about a broadband customer's use of the network for purposes such as marketing or advertising. In March 2017, Congress voted to disapprove the FCC's 2016 *Privacy Order* pursuant to the Congressional Review Act, which prevents the FCC from adopting another set of rules in substantially the same form.[13]

FTC Privacy Framework

Presently, all companies in the Internet ecosystem are subject to the Federal Trade Commission's privacy enforcement practice. The FTC privacy framework is technology neutral, and identifies categories of "sensitive" information that may give rise to an obligation by companies to obtain affirmative express customer consent (opt-in). Sensitive information includes: information about children, financial and health information, Social Security numbers, and precise geolocation data, according to the FCC.[14] Opt-in should be sought, for example, where a company's business model "is designed to target" consumers based on sensitive data, reasons the FTC, however risks to consumers may not justify the burdens that opt-in would entail for general audience businesses that "incidentally collect" sensitive information.[15]

---

[12] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Report and Order, 31 FCC Rcd 13911 (2016) (*Privacy Order*).
[13] *See* Pub. L. No. 115-22 (Apr. 3, 2017); *see also* 5 U.S.C. § 801(b)(2).
[14] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 47 (Mar. 26, 2012), *available at* http://go.usa.gov/csYRz
[15] *Id.*

Technology neutrality is appropriate, because as the FTC has observed, broadband providers (also referred to as Internet Service Providers, or ISPs) are no different than other participants in the Internet ecosystem in terms of their ability to collect and utilize information about consumers.

> ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.[16]

The FTC's recognition that opt-in should be limited is also appropriate. Consumers benefit from the use of information that companies see and collect in the course of serving their customers, as companies like Google have demonstrated. Advertising underwrites the cost of services that Google offers for free to the public, and there's no reason that advertising couldn't help offset the cost that broadband providers incur in offering broadband service (broadband providers should therefore be viewed as potential competitors to companies such as Google).[17] The *Privacy Order* would have foreclosed this possibility by requiring broadband providers to obtain opt-in approval to use customer data in the same manner as Google, although Google itself is under no similar obligation.

Opt-in typically results in substantially lower rates of consent than an opt-out system, because most of the time consumers take no action.[18] For example, in attempting to comply with the CPNI opt-in requirement, the former Regional Bell Operating Company U S WEST—at one time the primary provider of local exchange telephone service in 14 western states—obtained an

---

[16] *Id.*, at 56.
[17] "Google CEO sees free cell phone service," *Reuters* (Nov. 13, 2006) ("'Your mobile phone should be free,' Schmidt told Reuters. 'It just makes sense that subsidies should increase' as advertising rises on mobile phones."), *available at* https://www.reuters.com/article/businesspro-google-ceo-dc/google-ceo-sees-free-mobile-phones-funded-by-ads-idUSL0972867220061112.
[18] Huber, Fed. Telecom. Law, *supra* note 3.

opt-in rate of only 29 percent among it's residential subscribers at a cost of $20.66 per positive response.[19] Obtaining opt-in approval can be costly and inefficient compared to the alternatives (*e.g.*, inferred consent or opt-out consent, which do not require consumers to take action). Accordingly, it is anticompetitive if the most burdensome consent system is not applied equally to all market participants. Consumers are harmed when competition is lessened.

Different sets of rules for different firms (*i.e.*, asymmetrical regulation) can have anticompetitive consequences—or what the FCC chose to call "ripple effects" in the *Privacy Order* proceeding.[20] The goal should be to prevent regulations from hamstringing some market participants but not others, and the logical way to do that is by ensuring that all participants in the Internet ecosystem are treated the same. The FTC privacy framework, which applies to all participants in the Internet ecosystem, achieves this objective.

The *Privacy Order* justified asymmetric regulation on the ground that edge providers only get to see a "slice" of any given consumers Internet traffic, while broadband providers get to see 100 percent of a customer's *unencrypted* Internet traffic.[21] Encryption makes the Internet safer from eavesdropping, content hijacking, cookie stealing and censorship, according to the Electronic Frontier Foundation.[22] Encryption protected 77 percent of requests sent from computers around the world to Google's servers, for example, as of February 27, 2016.[23] By June 23 of this year,

---

[19] Thomas Lenard and Scott Wallsten, An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking, *Technology Policy Institute* at 27 (May 2016), *available at* https://techpolicyinstitute.org/wp-content/uploads/2016/05/Lenard_Wallsten_FCCprivacycomments.pdf (the authors observe that transactions costs like the ones incurred by U S WEST in this instance are "ultimately paid by consumers, either through higher prices or reduced services and benefits").

[20] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2546, para. 132 (2016) (*Broadband Privacy NPRM*).

[21] *Privacy Order*, *supra* note 12, 13920, para. 30.

[22] "We're Halfway to Encrypting the Entire Web," by Gennie Gebhart, Electronic Frontier Foundation (Feb. 21, 2017) *available at* https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web.

[23] "77 Percent of Google Internet Traffic Now Encrypted, by Angela Moscaritolo, *PC News* (Mar. 16, 2016) *available at* https://www.pcmag.com/news/342935/77-percent-of-google-internet-traffic-now-encrypted.

encryption protected 95 percent of Google's traffic.[24] Although not yet 100 percent pervasive across the entire Internet, particularly among smaller platforms, that's the direction encryption is heading. So in reality, the amount of a customer's encrypted Internet traffic that a broadband provider does not get to see is substantial, and the amount of unencrypted traffic it does get to see is shrinking. This is a perfect example of a market based solution that is eroding any justification for asymmetrical privacy regulation. The *Privacy Order* discounted encryption because it isn't 100 percent pervasive and ignored the fact that the use of encryption is clearly trending in that direction. Arguably, this is an example of government making unwarranted assumptions about how a dynamic market will evolve in order to pick winners and losers.

All participants in the Internet ecosystem gather valuable information in the course of serving their customers, and regulators will have to accept that the information that any particular participant, or class of participants, can gather may not be complete or identical to that which is available to other participants, and that in a perfect world companies would like to have direct access to all kinds of information that they do not. Markets are rarely perfectly competitive.

Rather than focus on the quantity and quality of customer information available to various market participants, the FCC in it's *Privacy* Order proceeding should have focused on whether there is, in fact, any harm to consumers from targeted advertising, and on how and why the existing FTC privacy framework may be unsuitable for broadband. The FCC had an obligation to set out why, from a consumer perspective, it's a materially more significant privacy threat for broadband service providers to know what websites a customer has visited, at what hours of day, from what location using which type of device than it is for a search engine to view search terms and click-throughs, and it failed to do so.

[24] "HTTPS encryption on the web," Google Transparency Report, *available at* https://transparencyreport.google.com/https/overview.

The Anticompetitive Purpose of Section 222.

When the FCC adopted CPNI rules in 1987, it specifically declined to adopt a "prior authorization" requirement like opt-in.[25] Sec. 222, enacted in 1996 in part to protect consumer expectations of privacy while facilitating information sharing between new entrants and incumbent providers who in most cases would be using many of the same facilities to serve their respective customers, but just as importantly—if not more so—it was "an important bulwark of the interconnection rules," designed to protect competing carriers from an "unscrupulous interconnector, also a competitor."[26] In particular, CPNI was intended to prevent the Regional Bell Operating Companies—who were the incumbent providers of local exchange service in most of the country, and who had traditionally not been permitted to offer long-haul interexchange toll (*i.e.*, long distance) services—from using billing data to "target the more lucrative long distance customers." The RBOCs were in possession of the data because they had provided billing services for the long distance carriers. The information became competitively useful to the RBOCs when they were finally allowed to offer their own long distance services. Long distance carriers felt it was anticompetitive for the RBOCs to be able to use customer information that would otherwise have been proprietary data belonging to the long distance carriers if the market had been competitive from the beginning. This is a competitor-focused perspective. Real consumer-focused privacy rules arguably would have allowed the RBOCs to immediately contact all of the lucrative long distance customers and offer them a better deal.

Requiring broadband providers to receive "opt-in" approval before they can use customer information for purposes such as targeted advertising, as the *Privacy Order* did, has only one

[25] Huber, Fed. Telecom. Law, *supra* note 3.
[26] Peter W. Huber, *et al.* The Telecommunications Act of 1996: Special Report (Aspen Law & Business, 1996), 54-55.

purpose and that is to make it harder for broadband providers to offer targeted advertising in competition with edge providers who would not have had to play by the same set of rules. Real consumer-focused privacy rules would not be aimed at protecting the competitors of the broadband service providers, but at ensuring that consumers can receive targeted ads from as many sources as possible. The Commission practices crony capitalism when it adopts rules that have the effect of picking winners and losers in the marketplace.

Investment Effect

The FCC argued during the *Privacy Order* proceeding that privacy regulation will *promote* broadband investment and deployment, because: a) the "largest investment ever in wireline networks came during those years in which DSL Internet access services were regulated under Title II," and b) "protection of privacy encourages broadband usage that, in turn, encourages investment in broadband networks."[27]

The second point is not the justification for new regulation that it may seem. If privacy protection encourages broadband usage and therefore promotes broadband investment, then broadband providers already have a natural incentive to protect privacy and FCC regulations are unnecessary.

The assertion that the largest investment in wireline networks occurred when DSL (*i.e.*, Digital Subscriber Line, or "dial-up," the technology that preceded broadband) was regulated under Title II is based on a flawed analysis by Free Press which looks at aggregate investment by incumbent and competitive local exchange carriers as well as wireless providers. Although all of these entities were covered under Title II, only the facilities of the incumbent local exchange carriers were subject to oppressive unbundling mandates that reduced incentives for investment in

[27] *Broadband Privacy NPRM*, *supra* note 20, 2505-06, para. 11.

last-mile facilities. Jeffrey A. Eisenach has observed that much of the pre-2000 investment was for marketing and operations, and that the elimination of unbundling in 2003-05 preceded an investment spike in broadband facilities.

> Since the FCC began exempting broadband infrastructures from unbundling requirements, overall investment in communications equipment in the U.S. has risen by more than 40 percent, as shown in Figure 2. And, unlike the prior investment bubble, much of which consisted of literally hundreds of billions "invested" by now bankrupt CLECs in advertising and overhead (Darby *et al* 2002), the bulk of the investment in the last five years has gone into network upgrades that have yielded a faster, more robust broadband infrastructure.[28]

The disastrous unbundling experiment that the Commission cited here—in which the Commission mandated artificially low prices for unbundled network elements that made it cheaper for new entrants to lease facilities from the incumbents rather than build their own, and which therefore required the incumbents to share any profits from successful investments and eat the entire loss from unsuccessful investments—illustrates why, for example, in the *Title II Order*, the Commission conceded that regulation can harm investment, and that "…deregulation often promotes investment…"[29] Moody's Investors Service also warned that broadband providers would be "severely handicapped" in their "ability to compete with digital advertisers such as Facebook and Google." The FCC disregarded this input when it adopted the *Privacy Order*, which buttressed the FCC's contrary conclusion on nothing more than an assessment by the National Consumers League that the industry had a strong financial year in 2015.[30]

Conclusion

Privacy regulation involves transaction costs and may have anticompetitive consequences if it is applied unevenly. Ideally, all market participants should be subject to a uniform privacy

---

[28] Eisenach, Jeffrey A., Broadband Policy: Does the U.S. Have it Right after All? (September 9, 2008). *available at* SSRN: http://ssrn.com/abstract=1265579.
[29] *Title II Order*, 5793-94, para. 414.
[30] *Privacy Order, supra* note 12, 13924, fn. 61.

framework administered by a single agency for the sake of consistency. The FTC's current privacy enforcement practice satisfies these criteria. Admittedly, making the Internet more secure will likely always be a work in progress, and there is a role for both market solutions as well as regulation.

Legislation to enhance consumer privacy protection, if any, should strive for technological and competitive neutrality. In particular, it isn't rational to subject some market participants to heightened *privacy* regulation just because they were subject to *economic* regulation in the past. We live in an era of rapid technological convergence, in which it is wise to consider that every participant in the Internet ecosystem is a potential competitor, at least to some extent. Moreover, privacy protection should be calibrated according to the sensitivity of the information at issue in recognition of the fact that there are transaction costs associated with consumer consent systems—opt-in systems are particularly burdensome and should be reserved for the only most sensitive personal information. Where customer information is less sensitive, consumer privacy expectations should be balanced with the benefits consumers are likely to derive from a dynamic, competitive market—where all providers have similar opportunities to innovate and earn a fair return on investment—including a greater abundance of choices and lower prices. Finally, to the extent possible, regulation should reflect the practical reality that it is difficult to make predictions about how the market will evolve and at what pace, and that the process of calibrating regulation on an ongoing basis as necessary to reflect changes in the market can be slow.