Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World

Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World

Harold Feld
Charles Duan
John Gasparini
Tennyson Holloway
Meredith Rose

A PK Thinks White Paper
February 2016

Published by:
Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036
http://publicknowledge.org

Cover image credit: Barett Lyon, the Opte Project, http://opte.org/maps/

Contents

Executive Summary

In February 2015, Federal Communications Commission (FCC) classified broadband Internet access service (BIAS)[1] as a Title II telecommunications service.[2] While largely exempting BIAS providers from the legal obligations of Title II carriers,[3] the FCC made a conscious decision to apply 47 U.S.C. § 222 — the section of the Communications Act that imposes a duty on Title II carriers to protect the "proprietary information" of their customers or interconnecting networks — to BIAS providers.[4]

At the same time, however, the Commission decided that it could not mechanically apply the existing § 222 regulations[5] — created as they were for the voice world — to BIAS providers. While the FCC recognized that consumers and competing businesses required protection of their proprietary data and confidential information in the broadband world just as they did in the voice world, it also acknowledged that the very different architecture and ecology of the broadband universe required special consideration. Accordingly, while the FCC applied the statutory duty of § 222 (and other relevant statutes this paper will explore) to BIAS providers, it did not apply the existing rules.[6]

---

[1] As discussed throughout this paper, it is important to distinguish between general, all-encompassing terms like "the Internet" and the very specific act of offering high-speed Internet access (generally referred to as "broadband"). Additionally, to understand the vital but narrowly circumscribed role of the FCC in this space, we must take great care to distinguish between services that offer a user access to "all or substantially all Internet endpoints" (a "broadband Internet access service" as defined by the FCC at section 8.11) and other services, such as the Amazon Kindle, which use the Internet to deliver certain limited functions (books, video) over the Internet. Accordingly, though cumbersome, this paper uses the technical term BIAS or BIAS provider to discuss the services and entities actually covered by the FCC's privacy authority.

[2] *In re* Protecting & Promoting the Open Internet, 30 F.C.C. Rcd. 5601 (Feb. 26, 2015).

[3] *Id.* at 5838–64 ¶¶ 493–536.

[4] *Id.* at 5616–17 ¶¶ 53–54.

[5] *Id.* at 5823 ¶ 467.

[6] *Id.* at 5820–4 ¶¶ 462–467.

Other than guidance issued to BIAS providers when the reclassification of BIAS to a Title II service went into effect in June 2015,[7] the FCC has provided no further official clarification of how it will enforce § 222 (and other provisions of the Communications Act relevant to privacy). As a result, the debate over how the FCC should address application of § 222 to BIAS providers has, unfortunately, proceeded with little deep discussion of the underlying statutory framework and how it differs from the general consumer protection framework employed by the Federal Trade Commission (FTC). Furthermore, the discussion has centered entirely on whether exsting protections for consumers are adequate, with no consideration of the equally important pro-competitive nature of § 222 and the FCC's overall mission to promote competition among competing services — a concern wholly different from that of the Federal Trade Commission.[8]

This white paper seeks to provide a general framework for the debate by exploring the statutory background of § 222 and FCC privacy jurisdiction generally. Without first understanding § 222 and how it works, both on its own and in conjunction with other section of the Communications Act, neither the FCC nor Congress can form coherent policy around application of these provisions to BIAS. Nor does it profit policymakers, or the stakeholder community at large, to debate the proper role of the FCC without understand the FCC's long history as a privacy regulator in the network environment.

Part I: The History of Section 222 and the FCC's implementation. Section 222 began in the Senate as a means of protecting competing local exchange carriers (CLECs) from the incumbent local exchange carriers (ILECs). It was the House that included an entirely separate section — which would become § 222 — focused on consumer privacy. Ultimately, the House and Senate conference compromise strove "to balance both competitive and consumer privacy interests." Understanding this dual nature of § 222 is critical to understanding why the language of § 222 speaks of "proprietary" information rather than "personal" information, and why

[7]Press Release, *Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy* (May 20, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0520/DA-15-603A1.pdf.

[8]Section 5 of the Federal Trade Commission Act empowers the FTC to prevent "unfair and anticompetitive trade practices." Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012). As we shall discuss further on, while the FCC general consumer protection statute (Section 201(b)) overlaps considerably with the FTC interpretation of Section 5, the FTC has no mandate to promote competition. Rather, the FTC plays a defensive role of preventing violations of antitrust.

Congress intended to convey especially broad powers to the FCC with regard to *both* competition and consumer protection.

For 20 years the FCC has enforced this dual mandate, including rules designed to address the growing problem of security breaches. Recently, the FCC has begun to expressly supplement its § 222 authority with other consumer protection provisions of the Act. Accordingly, Part I concludes with a review of other relevant provisions of the Communications Act the Commission must consider when formulating rules for BIAS providers.

Part II: The Relationship Between the FCC and the FTC. Nothing has generated so much confusion as the distinct roles of the Federal Communications Commission and Federal Trade Commission in protecting consumers. Part II therefore analyzes the statutory framework of the FTC, including how the FTC entered the privacy jurisdiction. The paper discusses the existing FTC statutory authority to protect consumer privacy. The FTC protects privacy as part of a broad consumer mandate, and does not actively promote competition via privacy policy. Its focus is thus complimentary to, and not in competition with, that of the FCC.

To the contrary, the FCC and the FTC have a long history of cooperation in a wide range of areas, including merger review, general consumer protection, and specific responsibilities in dealing with aggressive telemarketing under separate statutes directed to the FCC and FTC respectively.[9] Additionally, the FTC has similar concurrent jurisdiction over consumer protection matters and privacy issues with regard to other agencies.

Thus, contrary to industry arguments that FCC rulemaking would create conflict and confusion between agencies that would leave consumers unprotected,[10] such rulemaking with regard to BIAS providers is an intended part of the statutory scheme and a highly necessary function to promote competition and protect broadband subscribers. Indeed, were Congress to strip the FCC of its role in protecting privacy as some have proposed, it would result in a severe loss of protection for competitors and consumers alike. For the FTC to replicate the extensive specialized knowledge with regard to broadband networks and telecommunications practices needed to assume the FCC's historic role as a specialized privacy regulator would require dramatic expansion of the FTC's available

[9] *See infra* p. 40.

[10] *See, e.g.*, Letter from Am. Cable Ass'n et al., to Tom Wheeler, Chairman, Federal Communications Commission 2 (Feb. 11, 2016), *available at* https://www.ncta.com/sites/prod/files/Privacy_Letter_021116.pdf.

resources and engender significant disruption and confusion in the communications industry. By contrast, the purported benefits of stripping the FCC of its privacy authority appear both speculative and highly questionable.

Part III: Why We Need An FCC Rulemaking Just for BIAS Providers. Given this statutory framework, Part III considers the particular privacy concerns associated with BIAS providers that give rise to a need for an affirmative FCC rulemaking directed to those providers' practices, in order to protect consumers and promote competition. BIAS providers pose a unique and heightened risk to privacy for their subscribers, because of the unusually comprehensive and detailed data to which they have access in the course of offering broadband service. Internet data transmitted between subscribers and online services contain a great deal of information just in the routing information used to deliver that data to the correct destination. And BIAS providers who choose to engage in the practice known as "deep packet inspection" have an even larger wealth of information about their subscribers available to them. Providers can mine, analyze, and sell this rich consumer information to marketing companies and others, and subscribers have little technical recourse to prevent such privacy-invasive activity.

Lest this seem hypothetical, the paper continues on to identify numerous real-world examples in which broadband providers have engaged in exactly this type of consumer data collection and marketing. They have formed partnerships with marketing services, attached unremovable tracking beacons to subscribers' Internet transmissions, and even modified web pages accessed by subscribers to include advertising messages. The market for broadband subscriber information is so valuable — purportedly hundreds of millions of dollars — that in an ironic twist, providers have asked the FCC to refrain from privacy regulation so that those providers can avoid losing those profits.

The particularly comprehensive data that broadband providers enjoy gives them a distinct advantage over website operators and other online service providers, the so-called "edge providers." An edge provider receives only a subset of the information that a subscriber's online activity generates, and a subscriber can avoid edge provider data collection through a number of technical self-help means. By stark contrast, a BIAS provider receives *all* of a subscriber's online activity data, and the only way for the subscriber to avoid that data collection is to disconnect from

the Internet. Combined with the highly sensitive personal data that subscribers often must provide to obtain Internet access, these factors show that BIAS providers pose a special problem for consumer privacy, one that requires special attention from the FCC in the form of a rulemaking on § 222.

Part IV: What Should the Rules Say? In the final section, this paper takes all these factors together to make general recommendations on principles for a future FCC rulemaking or congressional action. The FCC must recognize the flexibility needed for Internet routing and — in accordance with the mandate of § 222 — allow consumers to agree to trade access to their personal information when desired. At the same time, the Commission must provide adequate protection not merely to consumers, but to competitors offering directly competing services, such as video or advertising, to BIAS providers. As Congress and courts have explained,[11] the FCC must respect the balance struck by Congress between empowering consumers to control their data and actively promoting competition by protecting the proprietary information that competitors must disclose to the BIAS provider.

Part IV begins by reaffirming the powerful framework for CPNI announced by the Commission in its 2007 CPNI Order.[12] As the Commission explained there, § 222(a), supplemented by 47 U.S.C. § 201(b), imposes a general duty on all carriers to protect the CPNI of consumers and competitors. Further, the Commission explicitly held that this general obligation included *any* sensitive "private personal information" that a carrier obtains by virtue of the carrier's relationship with the customer, and not merely the explicit categories listed in § 222(c).

As a first step, the FCC should clearly prohibit BIAS providers from interfering with user encryption or VPNs, and should affirmatively prohibit BIAS providers from using technologies such as deep packet inspection

[11] *See* Telecommunications Act of 1996, S. Rep. No. 104-230, at 205 (1996) (Conference Report) ("In general, the new section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI."); Verizon Cal., Inc. v. FCC, 555 F.3d 270, 273 (D.C. Cir. 2009) (noting that a carrier change request may be "proprietary information" under 47 U.S.C. § 222(b) because it provides a competitive advantage to the receiving carrier); *cf.* U.S.W., Inc. v. FCC, 182 F.3d 1224, 1236–37 (10th Cir. 1999) (observing congressional intent to balance competition and consumer privacy).

[12] *In re* Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking), *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009).

(DPI) for any use not permitted under the statutory exceptions for provision of service, protection of carrier property (harm to the network), or law enforcement. Because DPI exposes not only the information of the customer, but the information of other broadband subscribers to the BIAS provider, the FCC should find that a customer cannot consent to allow the carrier to see the content of a communication any more than a carrier could obtain consent to actively listen to an incoming phone call.

The FCC must also clarify that the duty to protect CPNI falls on the carrier, not the customer. Arguments that the availability of VPNs or encryption moot the need for strong rules protecting consumer privacy should be rejected as contrary to both the plain language of the statute and the framework adopted in the FCC's 2007 CPNI Order. Similarly, the FCC should make clear that the ability of non-carriers to collect similar types of information is utterly irrelevant to the duty imposed by Congress on all providers of telecommunications services — including BIAS providers — to protect CPNI.

Consistent with the Congressional intent to make customers the masters of their own information, the FCC must prohibit BIAS providers from coercing customer consent by disabling services or charging fees for privacy protections BIAS providers are required by law to provide. The FCC must carefully consider whether, and under what circumstances, BIAS providers may offer positive inducements, such as discounts, to customers to waive their tracking information. On the one hand, Congress affirmatively gave customers the right to access their own information and to consent to disclosure. This customer control must be respected. On the other hand, it is easy to see how prices can be set punitively high to coerce consumers, particularly the vulnerable poor, into accepting the "discount" to permit tracking.

In extending its CPNI framework to BIAS providers, the FCC should use all the statutory tools at its disposal, not merely § 222 and § 201(b). It should prohibit sharing CPNI between BIAS providers and their affiliates as a violation of § 222(b), 47 U.S.C. § 303(b), section 628(b) of the Cable Television Consumer Protection and Competition Act of 1992, and section 706(a) of the Telecommunications Act of 1996. Use of other customer information should require affirmative, informed consumer consent (e.g., "opt in" rather than "opt out"). Additionally, the FCC should retain its highly successful breach notification rules.

Finally, the Commission, Congress and all stakeholders should recognize that this complex and evolving area of law will require constant

revision in the next few years as technology evolves. It is not possible today to address all the potential threats and benefits of future information gathering technology. This complexity is not a reason to remain frozen with immobility as consumers and competitors suffer. To the contrary, it means that the FCC, after adopting rules to provide a basic framework, will need to continue to monitor industry developments going forward. The information and experience collected by the FCC will, in turn, inform the broader privacy debate.

Part I: The History of Section 222 and FCC Privacy Enforcement

A. Prior to the 1996 Act

During the 1970s and 1980s, the FCC began to promote what we would now call "over the top" services on the phone system.[13] Accepting the "natural monopoly" of the local telephone infrastructure (often referred to as the local "loop"), the FCC commenced a set of proceedings designed to encourage competition in the provision of end user equipment,[14] long distance,[15] the enterprise customer market for "private lines" that interconnect with the phone system,[16] and the market for "enhanced services."[17]

The FCC recognized that because competitors could only reach their customers by using the local phone system, it would need to take affirmative steps to prevent the local telephone company (technically referred to as the "incumbent local exchange carrier" or ILEC) from advantaging itself and interfering with its rivals. In proceedings similar to the recent net neutrality decisions, the FCC established structural rules to require ILECs not to discriminate against competing services,[18] to make information about their networks and network management transparent to com-

[13] Tim Wu, The Master Switch 188–91 (2010).

[14] *In re* Use of the Carterfone Device in Message Toll Servs., 13 F.C.C.2d 420 (1968).

[15] Wu, *supra* note 13, at 189; *see also* Alan Stone, How America Got Online 61–81 (1997).

[16] *In re* Petitions Seeking Amendment of Part 68 of the Comm'n's Rules Concerning Connection of Tel. Equip., Sys. & Protective Apparatus to Certain Private Line Servs., 76 F.C.C.2d 246 (1980).

[17] *In re* Regulatory & Policy Problems Presented by the Interdependence of Computer & Commc'n Servs. & Facilities, 7 FCC 2d 11 (1966) (Notice of Inquiry); *see also* Wu, *supra* note 13, at 190.

[18] Wu, *supra* note 13, at 190.

petitors,[19] and to require ILECs offering competing "over the top" services — such as alarm systems or dial-up Internet service — to offer such services through a separate affiliate.[20]

As this OTT competition became more established in the mid-1980s, the FCC discovered a further anti-competitive problem. Because providers of rival OTT services or rival facilities-based services (such as private lines or long-distance) could only reach customers through the ILEC, the competitor needed to provide the ILEC with an enormous amount of proprietary information on its customer base — such as the consumer's name, address, and the nature of the service purchased. The ILEC would also, of course, monitor the volume of traffic and the type of traffic passing over its system to the competitor, so that it could properly route traffic and bill the competitor.

As a result, the ILEC could convert the proprietary information of its OTT competitors into a virtual shopping list of potential clients for its own affiliates. It could convert its competitor's own business into market research. Worse from the standpoint of the competitor, the ILEC also had access to all other information on the calling habits of its customers, and the customers of all other OTT competitors. This gave the ILEC a huge advantage over any competitor, allowing it to bundle services and price packages in ways that targeted rivals and made competition impossible.

To illustrate by way of example, assume a landline phone customer of the early 1980s decided to subscribe to an alarm service offered by an independent company such as ADT. ADT would need to inform AT&T of the name and address of the customer, would need to hook its system into the customer's phone line (requiring ADT to also reveal information about what sort of technology it deployed), and the services ADT would provide to the customer. AT&T would also know how often the customer's burglar alarm went off. AT&T would know whether the customer called ADT regularly, and whether this represented an unhappy customer complaining or a happy customer upgrading, depending on whether ADT followed the call with an upgrade of equipment or additional services.

In addition to this information, AT&T would have a large trove of information about what other phone services the customer uses, and from this could deduce much about the subscriber's income and desirability as

[19]Policy & Rules Concerning the Furnishing of Customer Premises Equip., Enhanced Servs. & Cellular Commc'ns Servs. by the Bell Operating Cos., 95 F.C.C. 2d 1117 (1983) (Report and Order).

[20]Amendment of Section 64.702 of the Comm'n's Rules & Regulations ("*Second Computer Inquiry*"), 79 F.C.C.2d 953 (1980) (Memorandum Opinion and Order).

a customer. It could discern, for example, whether the subscriber calls a broker or bank regularly, or whether the subscriber frequently calls the helpline for state or federal benefits. AT&T could then pass all this information along to its alarm company affiliate, giving the AT&T alarm service affiliate an enormous advantage in trying to steal away ADT's customer, and giving that affiliate lots of market research to build a better alarm service to crush all competitors — all using the proprietary information competing alarm services must provide to AT&T by virtue of AT&T's role as the network operator needed to reach the customer.

To address this concern, the FCC adopted a series of orders prohibiting the local telephone provider from sharing proprietary information collected from rival OTT service providers with its affiliates and prohibiting use of the information collected as a phone service for any purpose *other than* providing the subscriber phone service.[21] When local telephone companies began offering competing mobile service, the FCC extended these rules to protect rival phone services.[22] These "non-accounting safeguards" would provide the origin of what we now call "Customer Proprietary Network Information," or CPNI.

B. The Legislative History of Section 222: A Combination of Competition and Consumer Privacy

With the Telecommunications Act of 1996, Congress intended to dramatically remake the telecommunications world by replacing traditional rate regulation of "natural monopoly" services with a structure based more on retail competition.[23] To do so, Congress intended to remove previous restrictions on incumbent providers (ILECs, cable companies) to compete in all lines of business with each other.[24]

But Congress did not intend to rely solely on "facilities based competition" between incumbent cable companies and incumbent telephone companies. Congress also envisioned a highly competitive "over the top" market in which existing OTT competitors (such as alarm systems) and

[21] *In re* Furnishing of Customer Premises Equip. & Enhanced Servs. by Am. Tel. & Tel. Co., 102 F.C.C.2d 655 (Sept. 30, 1985) (Order); *In re* Furnishing Customer Premises Equip. by the Bell Operating Tel. Cos. & the Indep. Tel. Cos., 2 F.C.C. Rcd. 143 (Jan. 12, 1987) (Report and Order).

[22] *In re* Implementation of the Non-Accounting Safeguards of Sections 271 & 272 of the Commc'ns Act of 1934, as amended, 11 F.C.C. Rcd. 21905 (Dec. 23, 1996) (First Report and Order and Further Notice of Proposed Rulemaking).

[23] Telecommunications Act of 1996, Pub. L. No. 104-104, pmbl., 110 Stat. 56, 56

[24] 47 U.S.C. § 253.

new entrants (such as competitive local exchange carriers) would provide services to customers by interconnecting with existing incumbents and having access to the necessary network elements to reach customers subscribing to incumbent services.

The drafters of the Telecommunications Act recognized that they faced the same problem with regard to proprietary information that the FCC addressed in the 1980s. To facilitate competition, Congress intended to let ILECs compete more freely in lines of business that the FCC previously restricted. But to ensue competition, the Telecommunications Act would need to protect proprietary information that competitors must reveal to incumbents in order to reach their customers.

1. The Senate Approach: A Focus on Protecting Information to Promote Competition

The Senate version of the Telecommunications Act of 1996, S. 652, essentially followed the approach of the FCC in focusing primarily on restricting the use of information collected by ILECs from competitors. S. 652 included restrictions on the use of proprietary information in 47 U.S.C. § 252, the section describing structural and non-accounting safeguards for competition in telecommunications services.[25] Specifically, proposed § 252(f) created:

> rules to ensure that the Bell companies protect the confidentiality of proprietary information they receive and to prohibit the sharing of such information in aggregate form with any subsidiary or affiliate unless that information is available to all other persons on the same terms and conditions.[26]

This did not mean that the Senate drafters were indifferent to consumer protection aspect of these privacy rules. As the conference report noted, the rule would generally prevent an ILEC from sharing any personal information "without the consent of the person to whom it relates."[27] The Senate Report also noted with approval the overall positive impact the provision would have on consumer privacy.[28] Nevertheless, as demonstrated by the limitation of this provision to ILECs and its overall placement as one subsection among other non-accounting safeguards,

[25] S. REP. NO. 104-23, at 22–24 (1995).
[26] *Id.* at 23–24.
[27] *Id.* at 24.
[28] *Id.* at 9.

it is clear that the Senate bill focused primarily on the pro-competitive aspect of what would become known as the CPNI rules, with consumer protection a secondary goal.

2. The House Approach: A Dramatic Shift to Consumer Protection

The House took a very different approach in its version of the Telecom Act, H.R. 1555.[29] The House bill completely reversed the focus of the Senate bill to focus primarily on consumer privacy protection, with competitive interests a secondary focus. H.R. 1555 created a new provision of the Communications Act entitled "Section 222 — Privacy of Customer Proprietary Network Information." The House bill separated the responsibility to protect CPNI as a "non-accounting safeguard" against the market power of existing incumbents into its own statutory section. New § 222 expanded the general duty to the Customer Premise Information of subscribers to *all* carriers, not just ILECs. As the House Report explained:

> All carriers are prohibited from using the information for any service other than the service from which it is derived or if it is necessary in the provision of customer premise equipment. These new privacy rules will apply to all telecommunications carriers — LECs, interexchange carriers and any other entity which offers services to the public generally (or to some segment of the public).[30]

The protections contained in §§ 222(b)–c represent a careful balance of competing, often conflicting, considerations. *First, of course, is the need for customers to be sure that personal information that carriers may collect is not misused*; this consideration argues for strict controls on a carrier's use of all customer data.[31]

---

[29]H.R. Rep. No. 104-204 (1995). Although H.R. 1555 passed on the House floor, it did not go to conference. Rather, after the Senate passed S. 652 and transmitted it to the House, the House adopted an amendment substituting the text of H.R. 1555 for the text of S. 652, then approved the new S. 652. This "amendment" of S. 652 (essentially an entire rewrite of the original) proceeded to conference, so that it was ultimately S. 652 (albeit a very different S. 652) that became law.

[30]H.R. Rep. No. 104-204, *supra* note 29, at 90.

[31]*Id.* (emphasis added).

The House Report also stressed that, in providing a definition of customer proprietary network information: "The term customer is intended to refer to the carriers' subscribers."[32]

Certainly the House Report also expressed concerns for promoting competition, just as the Senate Report had expressed concerns about the importance of consumer privacy. But the clear intent of both the changed legislative language and description of the intent of the new § 222 by the House Report demonstrates that, from the perspective of the House, protecting consumer privacy, enshrining the ability of consumers to control their information, and limiting the ability of carriers to use the information disclosed by subscribers to market them other products were the most important goal of the new § 222. Protecting consumer privacy, in the view of the House Report, was no longer a happy afterthought. Protecting consumer privacy should instead become the *primary* goal of CPNI and an independent goal of the Communications Act and the Federal Communications Commission.

It is important to note that this was not a completely radical change for the FCC. Congress had previously passed a strong privacy protection provision for cable subscriber information as part of the Cable Communications Policy Act of 1984, without any pro-competitive justification.[33] Additionally, the FCC always maintained its general consumer protection authority under § 201.[34] The effect of the House bill was to bring protection of subscriber policy more in line with these traditional consumer protection goals, and to subordinate the importance of promoting competition.

Section 104(a) of H.R. 1555, "Privacy of Customer Information," limited the new CPNI restrictions to "telephone service." Section 104(b), "Converging Communications Technologies and Consumer Privacy," required the FCC to do a study on the impact of converging media and communications technologies on consumer privacy.[35] The FCC would then report back to Congress to recommend further privacy regulation.

---

[32] *Id.* at 91.

[33] *See* Cable Communications Policy Act of 1984 § 631, 47 U.S.C. § 551.

[34] *See generally* Section I.D *infra* p. 19 (discussing application of 47 U.S.C. § 201 to CPNI).

[35] H.R. REP. NO. 104-204, *supra* note 29, at 22.

3. The Conference Strikes a Balance for the Telecommunications Act

The difference in the treatment of CPNI was hardly the only substantial difference between the Senate version and the House version of the Telecommunications Act of 1996. Integrating the two versions required a long and significant process, with many compromises between the Senate version and the House version.

The Conference Report stated that the final bill "strives to balance both competitive and consumer privacy interests with regard to CPNI."[36] As discussed in the next section, the final statutory language changed the FCC's traditional understanding of CPNI by making consumer privacy protection a primary goal, rather than a secondary goal. At the same time, the Senate negotiation in conference reconfirmed that the FCC should use this statutory authority for its historic purpose of actively promoting competition.

The effect of the conference, as discussed in more detail below, was to dramatically expand the *general* duty of carriers to protect customer information while significantly reducing the *specific list* of duties. The Conference changed the title of § 222 from "Privacy of Customer Proprietary Network Information" to "Privacy of Customer Information."[37] It now imposed a general duty to protect customer (and vendor) "proprietary information," followed by a specific limitations on the use of "customer proprietary network information."[38] It expanded the definition of CPNI to include all telecommunications services as opposed to specifically telephone service, and eliminated the FCC report on convergence.

As discussed in greater detail in the next section, the overall effect of the Conference report was to expand significantly the authority and flexibility of the FCC to create privacy rules to protect the privacy of subscribers to telecommunications services as the telecommunications environment evolved, without the need to return to Congress for separate authority. Similarly, the final bill made clear that while Congress now recognized the vital importance of protecting consumer privacy, Congress still intended the FCC to promote competition by protecting the proprietary information of competitors.

---

[36] S. Rep. No. 104-230, *supra* note 11, at 205.

[37] *Compare* H.R. Rep. No. 104-204, *supra* note 29, at 22, *with* S. Rep. No. 104-230, *supra* note 11, at 97.

[38] *See* S. Rep. No. 104-230, *supra* note 11, at 97.

C. Analysis of Section 222

With this background firmly in mind, we now analyze the relevant language of § 222, and the Commission's general interpretation of it over the years.

Section 222(a) begins with a general duty of all telecommunications carriers to protect the "proprietary information" of customers and other carriers. While on the one hand, this dramatically expands the responsibility to protect proprietary information from ILECs to all carriers, it also vastly truncates the list of responsibilities and duties of carriers from the comprehensive list in the House bill. However, the inclusion of the word "customer" in the language of § 222(a), in addition to the list of commercial entities whose information is protected, preserves the House intention that "the term 'customer' is intended to refer to the carrier's subscribers."[39] Otherwise, the list of covered entities in § 222(a) would be superfluous.

Section 222(b) is clearly a pro-competition provision, which limits the ability of telecom providers to use information disclosed by other telecom providers to provide competing service.

Section 222(c) defines a more specific class of proprietary information than that described under the general duty, namely "customer proprietary network information" (CPNI). It is within this context that the more extensive list of detailed limitations on carrier use of CPNI appears. Again, the final version both reduces the list of specific limitations contained in the House version, but expands the terms to have more general meaning.

Taken together, and applying the standard axioms of interpretation, the effect of these changes from the House to the final version is to provide greater flexibility, while enhancing the FCC's overall authority to protect the privacy of customer (and competitor) information. Congress recognized that it could not accurately forecast what specific information might become either personally or competitively sensitive in the future as communications technologies evolved and converged to include video service and other media. Rather than wait for Congress to do a study, Congress simply delegated the authority to the FCC to consider what rules, what type of information and what specific services should be covered over time. At the same time, Congress rooted this authority in the provision of "telecommunications services," the core of the FCC's jurisdictional expertise.

---

[39] H.R. REP. NO. 104-204, *supra* note 29, at 91 (describing 47 U.S.C. § 222(e)).

On the other hand, Congress had very clear concerns, driven in part by the experience of the FCC with CPNI prior to enactment, about certain specific types of information traditionally regulated as "Customer Proprietary Network Information," which Congress recognized needed immediate and specific limitations, beyond the mere general duty. Hence, while § 222(a) and § 222(b) apply to (and confer authority over) all information the FCC determines is generally "proprietary," Congress required additional and specific limitations on CPNI.[40]

Some have suggested alternate readings of § 222 such that subsections (a) and (b) would be effectively precatory to (c),[41] but the far better reading is that each subsection is an independent grant of authority as described above, for several reasons.

The general canons of statutory interpretation support this approach. As a general matter, when Congress uses a vague or indefinite term, this constitutes a direct delegation by Congress to "fill in the gaps" in interpretation.[42] Indeed, Congress's decision to name § 222 "Privacy of Customer Information" makes abundantly clear that Congress intended to broadly protect the privacy of consumers, consistent with the general duty of § 222(a). It also intended to impose a general duty to protect competition, through the general duty imposed by § 222(b). Because Congress had specific concerns about CPNI in addition to its general intent for the FCC to protect consumer privacy and competitive information, it required the FCC to impose specific restrictions on the use of CPNI *in addition to* any rules it found necessary to protect consumer privacy.

The structure of "general duty" with specific instructions with regard to subcategories appears several times in the Communications Act. This is hardly the only place in the Communications Act where the Commission imposes a general duty, then follows with specific instructions with regard to specific situations that raise particular concerns.

For example, the Cable Television Consumer Protection and Competition Act of 1992 added section 628 to the Communications Act, which

[40] *See* Verizon Cal., Inc. v. FCC, 555 F.3d 270 (D.C. Cir. 2009) (finding the word "proprietary" in 47 U.S.C. § 222(b) to have broader meaning than CPNI).

[41] *See* Petition for Partial Reconsideration of CTIA — The Wireless Association at 3–4, *In re* Lifeline & Link Up Reform & Modernization, Telecomms. Carriers Eligible for Universal Serv. Support, Connect Am. Fund, 30 F.C.C. Rcd. 7818 (Aug. 13, 2015) (WC Docket Nos. 11-42, 09-197, 10-90), *available at* http://apps.fcc.gov/ecfs/document/view?id=60001121721.

[42] City of Arlington v. FCC, 133 S. Ct. 1863 (2013); Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984).

generally prohibits cable and direct broadcast satellite (DBS) providers, or programmers affiliated with them (e.g., like NBC is affiliated with Comcast), from engaging in "unfair or deceptive practices, the purpose or effect of which is to hinder significantly or to prevent" a competing video provider from providing programming to "subscribers or consumers."[43] Section 628(c) contains specific instructions to the FCC with regard to programming networks affiliated with cable operators. For over 15 years, cable operators successfully induced a state of paralysis at the FCC by arguing that the general duty of section 628(b) was merely precatory language, leaving the far more limited section 628(c) as the only possible means by which the FCC could enforce the congressional intent to ban unfair and deceptive acts that undermined competition. Finally, in 2007, the FCC determined that Congress actually meant what it said in section 628(b) and banned a particularly blatant anti-competitive practice — signing exclusive deals with apartment building landlords to exclude competing video providers from their buildings.[44]

The D.C. Circuit rejected the argument from the cable industry that the more detailed list in section 628(c) preempted the broad general grant of authority in section 628(b).[45] To the contrary, as the court explained:

> Congress's enumeration of specific, required regulations in subsection (c) actually suggests that Congress intended subsection (b)'s generic language to cover a broader field. . . . Ultimately, then, our view of section 628's structure mirrors our view of its text: Congress had a particular manifestation of a problem in mind, but in no way expressed an unambiguous intent to limit the Commission's power solely to that version of the problem.[46]

Similarly, 47 U.S.C. § 225 of the Communications Act provides a general requirement in § 225(b) that the Commission make telecommunications services accessible to the deaf and hard of hearing "to the extent possible and in the most efficient manner." Section 225(c)–(d) prescribes specific services and regulations to be adopted with regard to existing

[43]Cable Television Consumer Protection and Competition Act of 1992 § 628(b), 47 U.S.C. § 548.

[44]*In re* Exclusive Serv. Contracts for Provision of Video Servs. in Multiple Dwelling Units & other Real Estate Devs., 22 F.C.C. Rcd. 20235 (Oct. 31, 2007) (Report and Order and Notice of Proposed Rulemaking).

[45]*Id.*

[46]*Id.* at 665.

telephone service immediately after enactment. No one has argued that § 225(c)–(d) are the sole limit of the Commission's authority to make all telecommunications services available to all the deaf or hard of hearing. 47 U.S.C. § 251(a) imposes a general duty to interconnect on all telecommunications service providers, whereas § 251(b)–(c) impose specific duties on incumbent local exchange carriers. No one seriously suggests, however, that the general duty to interconnect in § 251(a) is merely precatory, and the FCC is limited solely to the unbundling and interconnection agreements governing ILECs in § 251(b)–(c).

Finally, it is worth noting that while the Commission has, on occasion, used the word "proprietary" in § 222(a) as synonymous with CPNI in § 222(c), the Commission has, in those cases, expanded the definition of CPNI beyond the specific list of information provided for in § 222(c).[47]

D. Other Sources of Commission Authority To Protect Consumer Privacy

Finally, the FCC has long experience with both consumer protection and protection of privacy — particularly using its general authority under § 201(b) to require that all rates and practices "in connection with" offering a telecommunications service (such as broadband access) must be "just and reasonable." The FCC has used this section repeatedly in the last eight decades to protect consumers from anti-consumer practices.[48]

Because the Commission has recently begun to apply § 222 to broadband,[49] some have argued that reliance on § 201(b) for privacy is a novel

[47] *In re* Implementation of the Telecomms. Act of 1996: Telecomms. Carriers' Use of Customer Proprietary network Info. & Other Customer Info., 28 F.C.C. Rcd. 9609 (June 27, 2013) (Declaratory Ruling) (information that is reported by an app placed on the phone by the carrier is CPNI because the carrier has access due to customer relationship); *In re* Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927, ¶ 1, n.2 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking) ("CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services."), *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009).

[48] *See In re* Joint FCC/FTC Policy Statement for the Adver. of Dial-Around & Other Long-Distance Servs. to Consumers, 15 F.C.C. Rcd. 8654 (2000); *In re* Implementation of the Subscriber Carrier Selection Changes Provisions of the Telecomms. Act of 1996; Policies & Rules Concerning Unauthorized Changes of Consumers Long Distance Carriers, 15 F.C.C. Rcd. 8158, ¶ 19, n.47. (Apr. 13, 2000) (First Order on Reconsideration).

[49] *In re* Protecting & Promoting the Open Internet, 30 F.C.C. Rcd. 5601, 5616–17 ¶¶ 53–54 (Feb. 26, 2015).

interpretation and contrary to the statute.[50] History tells us otherwise, however. In adopting its rules on data breach notification in 2007, the Commission *expressly relied* on both its "general rulemaking authority under the Act," that is, § 201(b), and § 222(a), which imposes a duty on "[e]very telecommunications carrier . . . to protect the confidentiality of proprietary information."[51] Indeed, as noted earlier,[52] the original CPNI rules prior to enactment of the 1996 Telecommunications Act relied expressly on the Commission's § 201(b) authority.

Outside of Title II, the FCC has several other relevant sources of authority for regulating consumer privacy and protecting the proprietary information of consumers online, both directly and indirectly. We will touch on these briefly below.

1. Wireless Authority

In addition to regulating mobile broadband providers as Title II telecommunications service providers,[53] the FCC has broad authority to regulate wireless services generally under Title III of the Communications Act. For example, § 303(b) authorizes the Commission to make rules for any specific class of service — including mobile broadband service.[54] Section 303(r) requires the Commission to "make rules and regulations consistent with law" to carry out the purposes of the Communications Act and of any international agreements on telecommunications,[55] including

[50]Petition for Partial Reconsideration of CTIA — The Wireless Association, *In re* Lifeline & Link Up Reform & Modernization, Telecomms. Carriers Eligible for Universal Serv. Support, Connect Am. Fund, 30 F.C.C. Rcd. 7818 (Aug. 13, 2015) (WC Docket Nos. 11-42, 09-197, 10-90), *available at* http://apps.fcc.gov/ecfs/document/view?id=60001121721.

[51]*See Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info.*, 22 F.C.C. Rcd. ¶ 27, n.94 (citing 47 U.S.C. § 201(b) as general rulemaking authority deleted).

[52]*See* Section I.A *supra* p. 9.

[53]*Protecting & Promoting the Open Internet*, 30 F.C.C. Rcd. 5601.

[54]47 U.S.C. § 303(b).

[55]§ 303(r). The authority to implement international agreements may be particularly relevant here, in light of the recent agreement between the United States and the European Union on privacy. *See* Press Release, European Comm'n, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield* (Feb. 2, 2016), *available at* http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en; *see also* Natasha Lomas, *Europe And US Seal 'Privacy Shield' Data Transfer Deal To Replace Safe Harbor* (Feb. 2, 2016), http://techcrunch.com/2016/02/02/europe-and-us-seal-privacy-shield-data-transfer-deal-to-replace-safe-harbor/.

the requirement that all licenses issued serve the public interest, convenience and necessity.[56]

Even were mobile broadband providers not Title II telecommunications carriers and therefore exempt from "common carrier" regulation under what is called the "common carrier prohibition," these statutes would provide adequate authority for the FCC to protect the privacy of mobile subscribers and protect the proprietary information of businesses to promote competition.[57] As the D.C. Circuit has explained, the fact that a regulation also appears in Title II as a regulation of common carriers does not mean that it is inherently a "common carrier" regulation. Rather, for a rule to violate the common carrier prohibition, it must duplicate restrictions that are unique to common carriers and "relegate" the licensee to common carrier status.[58]

Rules governing disclosure of proprietary information, whether to protect consumer privacy or promote competition, are pervasive outside the realm of regulated common carriers. For example, as discussed in greater detail in Part II, the Federal Trade Commission has interpreted its general consumer protection statute to include basic privacy and cybersecurity protections.[59] Additional examples abound, including medical professionals,[60] financial institutions,[61] and even the legal profession.[62]

Consequently, even if the FCC did not have § 222 and § 201(b) at its disposal, it would have more than adequate authority to create rules to protect the privacy of mobile subscribers. Going forward, the FCC should not hesitate to invoke this additional authority.

2. Cable Authority

Since Congress passed the CCPA, the FCC has administered the highly restrictive privacy protections required under section 631 of that Act.[63] This statute is relevant here for two reasons. As an initial matter, it highlights the FCC's more than three decades as an agency specifically charged to protect consumer privacy. After 30 years of protecting the privacy of cable subscribers, and 20 years protecting the privacy of landline and mobile

[56]47 U.S.C. § 307(a).
[57]Cellco P'ship v. FCC, 700 F.3d 534, 549 (D.C. Cir. 2012).
[58]*Id.*
[59]FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
[60]42 U.S.C. § 17932.
[61]15 U.S.C. § 6801.
[62]D.C. Bar Association Rules of Professional Conduct 1.6.
[63]Cable Communications Policy Act of 1984 § 631, 47 U.S.C. § 551.

phone subscribers, the accusations of some detractors that the FCC lacks suitable experience in protecting consumer privacy to create privacy rules to protect BIAS subscribers rings somewhat hollow.

More directly, however, cable operators are the primary providers of broadband services — particularly at speeds of 25 Mbps or better.[64] Customers and competitors alike have legitimate concerns that cable providers will share information between their broadband affiliate and their cable affiliate — subjecting subscribers to invasive and predatory marketing practices and potentially discriminatory treatment based on stereotypical presumptions about race, age or gender.[65] As the FCC begins its examination of online privacy, it must pay particular attention to the relationship between bundled BIAS and video service.

3. Miscellaneous Provisions

The Communications Act has a number of miscellaneous provisions that potentially provide guidance and authority for the FCC as it assumes its proper role protecting privacy of BIAS subscribers. Two in particular bear mentioning. First, section 705(a) of the Communications Act of 1934 broadly disallows any carrier of a message to "divulge or publish" information about a communication "except through authorized channels" and only in limited situations.[66] It also states that "[n]o person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[67]

Second, section 706(a) requires the FCC to take affirmative steps to encourage the deployment of "advanced telecommunications services" to all Americans.[68] As the Commission found in 2007 with regard to interconnected VOIP services, "protection of CPNI may spur consumer demand . . . driving demand for broadband connections, and consequently encouraging more broadband investment and deployment consistent with Section

---

[64] *See In re* Deployment of Advanced Telecomms. Capability to All Americans in a Reasonable & Timely Fashion, GN Docket No. 15-191 (Jan. 29, 2016) (2016 Broadband Progress Report).

[65] *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 100–01 (2014) (describing how big data collection and analysis can be used to effect racially discriminatory practices).

[66] Communications Act of 1934 § 705(a), 47 U.S.C. § 605.

[67] *Id.*

[68] Telecommunications Act of 1996 § 706(a), 47 U.S.C. § 1302.

706."[69] This reasoning is only further reinforced by research by the Pew Research Center[70] and others. Americans feel that they have lost control of their privacy online. The inability to trust that one's broadband provider will respect the privacy of personal information is one of several barriers to consumers increasing use of broadband services, undermining the virtuous cycle of increased consumer demand stimulating greater investment in deployment and availability of higher speeds.

E. Conclusion

The above list of additional statutory authorities is not intended to be exhaustive. Other statutes and sources of authority may well apply. Rather, this analysis of the history of CPNI and § 222, combined with discussion of other consumer protection provisions of the Communications Act, should provide a necessary legal foundation for the FCC's role in protecting to the privacy of subscribers to broadband Internet access services and the additional important role of affirmatively promoting competition by protecting the proprietary information of service competitors.

This history and general review of the statutory mandates, taken together, show that the FCC has considerable experience in the realm of protecting consumer privacy in communications networks. Extension of privacy protection to BIAS subscribers continues the natural evolution of protecting consumer privacy over the last 30 years for cable subscribers, telephone subscribers, and mobile phone subscribers. Rather than a rash adventure into unproven ground, FCC action to protect the privacy of BIAS subscribers is the specific obligation of the FCC to keep pace with the evolution of communications technology.

In the next section, we will discuss the relationship between the Federal Communications Commission privacy enforcement and the privacy enforcement of the Federal Trade Commission. As the more than 30 years of FCC responsibility for protecting subscriber privacy in cable, telephone, and cellular services suggests, joint jurisdiction between the two agencies for consumer protection of privacy does not exactly break new ground. Nor, as we will discuss more extensively in the next section, is privacy the

[69] *In re* Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927, ¶ 59 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking), *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009).

[70] Mary Madden, Pew Research Ctr., *Privacy and Cybersecurity: Key findings from Pew Research* (Jan. 16, 2015), http://www.pewresearch.org/key-data-points/privacy/.

only area where the FCC and the FTC have complimentary jurisdictions — or where the FTC shares jurisdiction for privacy with other agencies (including other agency regulators of common carriers).

Part II: Complementary Roles of the FCC and the Federal Trade Commission

Nothing has raised greater confusion in the debate on the proper role of the FCC in protecting the privacy of BIAS subscribers than the complementary role of the Federal Trade Commission (FTC). As Commissioner Julie Brill recently observed, shared jurisdiction between the FTC and the FCC on a number of consumer protection issues, as well as shared jurisdiction between the FTC and other agencies with regard to privacy specifically, is hardly new.[71] To the contrary, the FTC has a long history of working cooperatively with specialized agencies such as the Food and Drug Administration,[72] and well as agencies regulating financial institutions.[73]

Nevertheless, the long history of interagency cooperation with the FCC and other agencies on consumer protection and privacy matter has not prevented numerous critics from challenging the role of the FCC in protecting consumer privacy. This criticism generally takes the form that the Federal Trade Commission is "the" privacy protection agency, and therefore – for simplicity and to create a "level playing field" between broadband access Internet service (BIAS) providers and online content

[71] *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Address at the Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality: Net Neutrality and Privacy: Challenges and Opportunities (Nov. 19, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/881663/151119netneutrality.pdf ("Where the FTC and FCC overlap in other enforcement areas, we have long had a successful working relationship.").

[72] Sarah E. Taylor & Harold J. Feld, *Promoting Functional Foods and Nutraceuticals on the Internet*, 54 Food & Drug L.J. 423, 440 (1999).

[73] Fed. Trade Comm'n, How to Comply with the Privacy of Consumer Information Rule of the Gramm-Leach-Bliley Act (2002), https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

and service providers – the FCC should vacate the field of privacy protection in favor of jurisdiction by the FTC.[74]

Setting aside the industry agenda, however, consideration of the proper relationship between the FCC and the FTC in protecting consumer privacy is critical for the FCC to create an effective framework to ensure that consumers enjoy appropriate protection from BIAS providers, ensure competition between over-the-top (OTT) providers competing with BIAS provider OTT affiliates, and avoid interference with the FTC's proper role in protecting consumer privacy online. Fortunately, as discussed in greater detail below, the FCC and the FTC have already concluded an interagency memorandum of understanding on the subject,[75] modeled after the memorandum between the Consumer Financial Protection Bureau and the FTC.[76]

As demonstrated below, the FTC has a very different statutory framework for protection of privacy. Unlike the FCC's "narrow but deep" statutory framework for privacy protection, the FTC must cover a very broad set of industries with a very generic consumer protection statute. As a consequence, the FTC relies on specialized agencies such as the FCC to apply their additional expertise and statutory authority where applicable. To understand how these different statutory regimes work together, this white paper will first trace the history of the FTC, with an emphasis on its evolving role in privacy and cybersecurity protection. It will next compare this to the unique role of the Federal Communications Commission, demonstrating why efforts to force the FTC to handle online privacy alone would undermine both consumer protection and promotion of OTT competition. It concludes with an analysis of the history of FCC/FTC competition. Part IV, the section on general recommendations to the FCC as it proceeds to a notice of proposed rulemaking, will discuss how it should

[74]Indeed, industry advocates have long advocated for Congress to strip the FCC of its longstanding jurisdiction over cable and voice privacy, as well as its jurisdiction over broadband privacy. *See* James Robinson, *The 21st Century Privacy Coalition Doesn't Really Care About Your Privacy*, PANDO (June 4, 2014),/2014/06/03/despite-team-up-for-the-21st-century-privacy-coalition-americas-telecoms-giants-really-arent-looking-out-for-your-privacy/. It goes beyond the scope of this paper to rebut these arguments thoroughly.

[75]Memorandum of Understanding from Fed. Commc'ns Comm'n & Fed. Trade Comm'n (Nov. 16, 2015) [hereinafter FCC-FTC Memorandum of Understanding], http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf.

[76]Memorandum of Understanding from Fed. Trade Comm'n & Consumer Fin. Prot. Bureau (Mar. 6, 2015), *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/150312ftc-cfpb-mou.pdf.

structure its own rules to properly reflect both the experience of the FTC in broadband and the ongoing cooperation between the two agencies.

A. The General Structure of the FTC and Its Relationship with Other Federal Agencies

As we shall examine in greater detail below, the FTC sits at the center of a "hub and spoke' design for consumer protection. Under section 5,[77] the FTC generally protects consumers from "unfair and deceptive" practices, subject to certain statutory limitations. Specifically, the FTC must as a general matter proceed by enforcement, not by rulemaking.[78] In other words, the FTC must bear the burden of proving that a specific practice by a specific company is "unfair and deceptive," rather than having a broader rulemaking to determine, for example, if certain uses of private information are intrinsically unfair and deceptive. This enforcement mechanism is further limited by section 5(n), which requires the FTC to show that the consumer could not have otherwise avoided the injury and that there are no other offsetting advantages to competition.

In jurisdictions where Congress has determined that additional oversight is necessary, Congress has directed other agencies to exercise consumer protection (and in some cases, explicitly privacy) jurisdiction. This reflects Congress's general determination that these specific markets or areas of concern, for example medical privacy, regulation of food and drug safety, financial regulation, and — most relevant here — communications, have specialized agencies that work alongside the FTC.[79] These special markets share certain common features. Notably, they require unique expertise (either technical or of the specific market structure, or both), they generally have an obligation to serve the public interest rather than simply the private interest, they are prone to concentration, and the consequences of a failure in these markets can be catastrophic for either individual consumers or the national economy as a whole.

There is no doubt that the FTC's general privacy jurisdiction needs significant expansion and improvement to fulfill its function. The rise of platforms such as operating systems, search engines, or social media companies that can use technology to track individuals at the most granular level raises grave concerns for the future of consumer privacy. If the FTC is to protect consumer privacy in a market where consumers must

[77] Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012).

[78] *See generally* discussion *infra* note 86.

[79] *See* examples *infra* p. 41.

guard their private conversations from their televisions[80] or their other "smart devices,"[81] then Congress must enhance the FTC's authority to address these threats to consumer privacy, as well as the resources to address them.

Giving the FTC authority to do its job, however, is a very different question from whether the FTC should take over the jobs of other agencies in the current "hub and spoke" structure created by Congress. Here, the answer is firmly "no." Just as HHS should continue to police privacy in the medical profession while leaving devices that collect medical data to the FTC, so to should the FCC continue to play its proper role in protecting proprietary information of both consumers and competitors from BIAS providers.

B. The History of the FTC's Privacy Jurisdiction and the Common Carrier Exemption

Unlike other countries, the United States does not have a single privacy law or a single agency tasked with protecting privacy. To the contrary, the United States has a patchwork of privacy laws, generally directed at specific industries and agencies.[82] How, then, did the FTC acquire the general jurisdiction as the general protector of consumer privacy in the digital age?

Congress created the Federal Trade Commission with passage in 1914 of the FTCA.[83] Originally intended to police "unfair methods of competition" (*i.e.*, antitrust), Congress expanded the Commission's authority under section 5 of the FTCA to prohibit "unfair or deceptive acts or practices."[84] While Congress has amended the FTCA over the years to add additional statutory authority, section 5 forms the core of the FTC's consumer protection authority.[85]

---

[80] *See* Chris Matyszczyk, *Samsung's Warning: Our Smart TVs Record Your Living Room Chatter*, CNET (Feb. 8, 2015), http://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/.

[81] Ms. Smith, *Security and Privacy Checklist for Smart Home, IoT Devices*, NETWORK WORLD (Dec. 9, 2015), http://www.networkworld.com/article/3013512/security/security-and-privacy-checklist-for-smart-devices-50-million-to-be-sold-over-holidays.html.

[82] *See, e.g.*, 42 U.S.C. § 17932 (medical records); 15 U.S.C. § 6801 (financial); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505 (online services directed to children).

[83] Federal Trade Commission Act of 1914, ch. 311, sec. 5, 38 STAT. 717, 719.

[84] Wheeler-Lea Act of 1938, ch. 49, sec. 3, § 5(a), 52 STAT. 111, 111–12.

[85] *See* Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012).

1. The FTC's General Enforcement of Section 5 and Role In Protecting Privacy

As a general matter, the FTC does not implement its consumer protection through rulemaking.[86] Rather, "enforcement functions as the core" of the FTC's operations,[87] by which the agency gathers evidence to issue a complaint and uses settlement decrees or litigation to force companies to discontinue anti-consumer practices and to make recompense to injured consumers.

Outside consumer credit and financial reporting, consumer privacy — especially privacy of consumer information gathered by companies providing online services — remained a largely underappreciated area of concern.[88] Following the passage of statutes in the 1990s addressing consumer privacy protection in the realm of health services, financial services, and protecting children's privacy online,[89] the FTC began to take a more active role with regard to privacy protection generally — especially with regard to consumer data collection by businesses online.[90] In the absence of any federal statute specifically granting the FTC authority over online privacy, the FTC has applied its general consumer protection enforcement power to include privacy and, more recently, cybersecurity.[91]

---

[86]Occasionally, Congress does require the FTC to engage in specific rulemakings. These provisions, including the rather narrow rulemaking Congress required under the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505, do not impact the general analysis of overall relevant FTC authority. The FTC could theoretically make general rules under its section 5 authority, *see* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 697–98 (D.C. Cir. 1973), but Congress has imposed stringent requirements on the FTC's rulemaking procedure, *see* Magnuson-Moss Warranty Act, Pub. L. No. 93-637, sec. 202, 88 STAT. 2183, 2193 (1975), *codified at* 15 U.S.C. § 57a; Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, secs. 7–12, 94 STAT. 374, 376–78 (amending same). In the face of these requirements, the FTC has not engaged in a single new section 5 rulemaking since 1980. *See* Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1989 (2015). There is little reason to believe it would change course on BIAS provider privacy, and so that possibility is not considered likely in this paper.

[87]Edith Ramirez, Chairwoman, Fed. Trade Comm'n, *The FTC: A Framework for Promoting Competition and Protecting Consumers*, 83 GEO. WASH. L. REV. 2049, 2054 (2015).

[88]*See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 3–6 (2010) [hereinafter FTC 2010 PRIVACY REPORT], *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

[89]*See* statutes cited *supra* note 82.

[90]*See* FTC 2010 PRIVACY REPORT, *supra* note 88, at 3–6.

[91]*See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012) [hereinafter FTC 2012 PRIVACY REPORT], *available at* https://www.ftc.

Because the FTC lacks both effective rulemaking authority and specific power from Congress to develop standards to protect consumer privacy specifically, the FTC is constrained by the limits of section 5 to apply the same, general "unfair and deceptive" standard to online privacy issues as it does to other business practices. While in part that involves enforcement actions against broken privacy promises, the Commission may also conclude that a practice falls so far below what a reasonable consumer may expect, or is so burdensome for a consumer to discover, that it is "inherently unfair."[92] Such determinations, however, must be made with reference to general industry practices, rather than based on the FTC's judgment as to what practices would best protect consumers.[93]

Finally, section 5 on its own terms prohibits the FTC from applying section 5 to a variety of entities, including "common carriers subject to the acts to regulate commerce." The term "common carriers" pursuant to that section includes a wide variety of businesses and entities.[94] Of relevance here, the FCC's classification of broadband as a Title II service places broadband providers squarely within the category of common carriers, and thus outside the general scope of section 5 of the FTCA.

2. The Common Carrier Exception

Both the original 1914 Act creating section 5, and subsequent amendments such as the Wheeler-Lea Act of 1938, prohibited the FTC from regulating "common carriers subject to the Acts to regulate commerce."[95] Telephone companies were already regulated as common carriers in 1914 under the authority of the Interstate Commerce Commission (ICC) under the Mann-Elkins Act of 1910.[96] At the time of the Wheeler-Lea Act of 1938, telephone services were common carriers regulated by the FCC under the Communications Act of 1934.[97]

---

gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015).

[92] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 627–43 (2014).

[93] FTC 2012 PRIVACY REPORT, *supra* note 91, at 38.

[94] *See, e.g.*, FTC v. Verity Int'l, Ltd., 443 F.3d 48, 56–60 (2d Cir. 2006).

[95] Federal Trade Commission Act § 5(a)(2), 15 U.S.C. § 45 (2012).

[96] *See* Mann-Elkins Act of 1910, ch. 309, sec. 1, 36 STAT. 539, 539.

[97] Communications Act of 1934, ch. 652, sec. 3(10), 48 STAT. 1064 (defining "common carrier" as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy").

The origins and persistence of the "common carrier" exception to the FTC's authority remain subject to considerable debate and go well beyond the scope of this paper. Sufficient for our analysis are the following. First, the FCC and the FTC have a history spanning more than 80 years creating a long standing framework for cooperation which we will address in greater detail below. Second, the FTC has no particular expertise in regulating the privacy of networks.

C. Comparing the FCC and the FTC: Complementary Roles Vital To Consumer Protection

It has become almost a cliché in regulatory circles to argue whether the FCC or the FTC is "best" suited to protect privacy.[98] This is rather an absurd argument. Protecting consumer privacy — online and off — is a complex issue involving a variety of specialized agencies working in harmony with the Federal Trade Commission to provide a basic level of protection for consumers across all services. This is not some trivial argument as to whether Superman or Batman is the better hero or whether the monsters from the "Aliens" movie franchise can beat up the monsters from the "Predators" movie franchises.

Neither the FCC nor the FTC has the statutory authority or resources to regulate "online privacy" independently. Rather, both the FCC and the FTC have unique responsibilities to address the overall goals of protecting consumer privacy and OTT competition.

1. The FCC's Unique Pro-Competition Perspective and Pro-Consumer Rulemaking Authority

As noted extensively in Part I, the FCC has a long history of using its privacy protection as an affirmative tool to promote competition.[99] Congress expressly required the FCC to adopt this role when Congress imposed on telecommunications providers a duty to protect not only the proprietary information of customers, but of competitors.[100] By contrast, the FTC reg-

[98]Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, Address at the 33rd Annual Institute on Telecommunications Policy & Regulation: FTC-FCC: When Is Two a Crowd? (Dec. 4, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/893473/151204plispeech1.pdf ("D.C. is abuzz with talk about FTC and FCC jurisdiction over privacy and data security.").

[99]*See* Part I *supra* p. 9.

[100]*See* 47 U.S.C. § 222(a)–(b).

ulates privacy solely through its consumer protection authority.[101] Without additional protection from the FCC, consumers would suffer both a general loss of overall competition in competing services, and intrusive marketing practices on the part of broadband providers.

More importantly, section 5(n) of the FTCA, adopted by Congress in 1994, severely restricts the ability of the FTC to act to protect consumers (let alone competition), as compared to the FCC. section 5(n) requires that for the FTC to declare an act or practice "unfair," it must first find that the action "causes, or is likely to cause, substantial injury to consumers." Furthermore, the FTC must consider whether the consumer could have otherwise avoided the injury, or whether there are offsetting advantages to consumers and competition generally.[102] Further, while the FTC can consider existing industry best practices, mere violation of these practices cannot, in themselves, constitute an unfair practice.[103] Since the FTC must proceed through enforcement actions on a case-by-case basis, the FTC cannot easily set rules for specific industries or respond nimbly to changed circumstances in a particular area — especially one as concentrated and specialized as broadband access.[104]

By contrast, Congress has explicitly told the FCC to create rules to protect consumer privacy for telecommunications services — which now include BIAS services. Additionally, Congress has provided the FCC with copious authority to protect consumers and enhance competition, as discussed at considerable length in Part I.

The abilities of the FTC and the FCC to respond to growing concerns that companies possessing consumer information fail to take appropriate measures to protect this information, and to require companies to inform consumers when their personal information is released without authorizations ("data breach notification"), illustrate the difference between the FTC's general authority through enforcement and the FCC's rulemaking authority.

---

[101] *See* FED. TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION POLICY 38–41 (2007), https://www.ftc.gov/reports/broadband-connectivity-competition-policy-staff-report.

[102] *See* Federal Trade Commission Act § 5(n), 15 U.S.C. § 45 (2012) (discounting injury to consumers "which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition").

[103] *See id.* ("Such public policy considerations may not serve as a primary basis for such determination.").

[104] *See* FTC 2012 PRIVACY REPORT, *supra* note 91, C–7 (Rosch, Comm'r, dissenting).

Data Breach, Cybersecurity. The FTC, while recognizing concerns for cybersecurity in its 2012 *Privacy Report*, has no effective authority to issue regulations to require companies to take precautions against exposure of customer data, or to require businesses to notify providers in the event of a breach. Only in August 2015 did the Third Circuit affirm, in *Wyndham Worldwide*, the FTC's ability to hold businesses to comply with basic cybersecurity precautions.[105]

Almost immediately, a decision by an FTC Administrative Law Judge demonstrated the enormous difficulty consumers would find in seeking relief from the FTC under the *Wyndham Worldwide* decision. In *In re LabMD, Inc.*, the FTC filed a complaint alleging that LabMD had failed to take even elementary precautions to protect its customer data, resulting in the personal data — including social security numbers and other highly sensitive financial and health data — making its way on to peer-to-peer information networks.[106] Nevertheless, the ALJ found that the FTC had failed to meet its burden of showing substantial consumer harm under as required by section 5(n).[107]

Although the FTC has appealed internally within the agency, it will take some considerable time for the case to resolve — especially if LabMD appeals an adverse ruling. Even if the FTC is ultimately successful, it will not establish a rule binding on all industries subject to the FTC's jurisdiction. Instead, it will provide precedent for future enforcement actions.

Gradually, as the precedent becomes more firmly established, businesses will respond. But the nature of the FTC's enforcement process, including the limitations imposed by section 5(n), make it exceedingly difficult for the FTC to address the factors that make BIAS providers unique.

FCC Rapid Response and Rulemaking. By contrast, because the FCC has general rulemaking authority and a narrow focus on telecommunications providers, the FCC was able to respond swiftly and on an industry-wide basis when confronted in 2005 with a petition from the Electronic Privacy Information Center (EPIC) to adopt new rules to protect CPNI.[108] The FCC sought public comment on the Petition and adopted

---

[105] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 249 (3d Cir. 2015).

[106] *See In re* LabMD, Inc., No. 9357, slip op. at 1–2 (FTC Nov. 13, 2015) (on appeal to Commission), *available at* https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.

[107] *See id.* at 87–88.

[108] *See In re* Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927, ¶ 2, n.5 (Apr. 2, 2007) (Report and Order and Further

sweeping new rules in 2007 to protect consumers from the growing problem of "pretexting;" practices by which identity thieves collected personal information from phone carriers leveraging publicly available information. In doing so, the Commission also relied on recently passed legislation criminalizing pretexting, and the Congressional findings on the threat to the physical safety, as well as the economic well being, of consumers whose personal information had been stolen by pretexters.[109]

Unhampered by the restraints of proceeding through case-by-case enforcement, the FCC enacted sweeping rules on traditional telephone providers, wireless providers and providers of interconnected voice-over-IP services to protect the privacy of customer information.[110] These included mandatory security precautions,[111] mandatory data breach notification,[112] annual compliance reporting,[113] and an "opt in" requirement for carriers to share information with joint venture partners or third-party contractors.[114] Unlike the FTC's case-by-case approach exemplified in Wyndham, the FCC's rules became applicable on an industry-wide basis after publication in the Federal Register.[115]

2. The FCC Has Unique Expertise, and Must Balance Consumer Privacy Among the Multiple Goals of the Communications Act

The FCC has an already-developed deep understanding of the broadband industry. Such an understanding is essential not merely for privacy enforcement, or consumer protection generally. As the expert agency on communications, it is impossible for the FCC to perform its functions

---

Notice of Proposed Rulemaking), *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009).

[109]Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records." *See id.* ¶ 1, n.1. The FCC noted that "Congress has responded to the problem by making pretexting a criminal offense subject to fines and imprisonment." *Id.* (citing Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 STAT. 3568 (2007)); *see also id.* ¶ 44 (quoting congressional findings of that statute).

[110]*See id.* app. B (amending 47 C.F.R. §§ 64.2003–.2011). "Interconnected VOIP" is a service that allows users to communicate two-ways in real time, and must have the capability to reach standard phone numbers on the traditional telephone network. *See id.* ¶ 54, n.170.

[111]*See* 47 C.F.R. § 64.2009.

[112]*See* 47 C.F.R. § 64.2011.

[113]*See* 47 C.F.R. § 64.2009(e).

[114]*See* 47 C.F.R. § 2010.

[115]*See* Customer Proprietary Network Information, 72 Fed. Reg. 31948, 31948 (FCC June 8, 2007). Some of the rules required approval of OMB and were thus made effective at a later date. *See id.*

without a basic understanding of how the broadband industry works. This extends well beyond consumer protection or privacy. The FCC administers the National Broadband Plan, it is in the midst of transitioning the telephone system to an all IP-based platform, it is restructuring the system of federal subsidies that currently support telephone service to redirect them to support broadband service. The FCC, in its various component programs, spends the vast majority of its time and resources understanding the broadband industry and trying to move the industry in a direction that enhances competition and promotes affordability and innovation.

The FCC's expert knowledge is critical to formulating sustainable privacy rules. First and foremost, the FCC has a twin mandate to protect consumers and to promote OTT competition. An understanding of the broadband industry must inform the FCC's rulemaking to address these twin goals. In addition, the FCC must properly balance concerns about the exchange of necessary information for routing and traffic exchange – problems similar to those the FCC addressed in the traditional telephone world.

By contrast, the FTC covers a broad range of businesses. Indeed, it is easier to list what the FTC does not cover under its section 5 consumer protection jurisdiction. As a consequence, when the FTC decides to bring an enforcement action, it must develop specific expertise for the complaint – particularly in light of the requirements of section 5(n).

It is not that the FTC couldn't, given sufficient resources, eventually replicate the expertise the FCC already has. But why bother to recreate the FCC when the FCC already exists? Furthermore, whereas the FCC has an explicit statutory mandate to consider whether providing subscribers and competitors with privacy protections will contribute to investment and deployment in new broadband infrastructure and service,[116] the FTC has no capacity — or authority — to consider how its enforcement would impact our national policy of promoting competition among competing services and ensuring that consumers enjoy adequate protection in the deployment of critical communications service. To the contrary, the limitations imposed by the FTC by section 5(n) preclude such detailed and nuanced balancing to ensure the public interest.

[116] *See* Telecommunications Act of 1996 § 706, 47 U.S.C. § 1302, *interpreted by In re* Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927, ¶ 59 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking), *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009).

Case study: Verizon "Supercookie." In the fall of 2014, the Electronic Frontier Foundation (EFF) documented that Verizon Wireless was inserting a means of tracking their wireless broadband subscribers Internet browsing habits by injecting a special identifier into their bit-stream.[117] Verizon used the inserted tracking identifier to assist third parties in obtaining customer data from Verizon's expanding online advertising program. Problematically, though, the identifier could also be used, independent of Verizon's advertising program, to track a user across multiple website visits. It thus acted much like the known technology of web cookies, but with a catch: although customers could "opt out" of the advertising sharing, customers could not opt out of having the tracking identifier inserted in their Internet traffic.[118] This gave rise to the popular names "supercookie" or "zombie cookie" because users could not use conventional means to avoid tracking (as opposed to cookies used by third party entities such as Google or Facebook, which can be cleared or rejected by the user).

EFF warned readers that only by using security measures that require either technical proficiency or additional fees (or both) could Verizon subscribers avoid the Verizon supercookie. Standard encryption and standard practices for clearing the tracking software were not sufficiently effective to prevent Verizon (or others) from tracking Verizon subscribers.[119]

Several deeply disturbing facts quickly came to light. First, despite Verizon's initial claims that third parties could not access the information without Verizon's consent, it turned out that third parties could read the injected header without Verizon's permission and thus gain information about Verizon's subscribers, even if Verizon's subscribers had explicitly opted out of the tracking program.[120] Second, although Verizon started

[117] *See* Robert McMillan, *Verizon's 'Perma-Cookie' Is a Privacy-Killing Machine*, WIRED (Oct. 27, 2014), http://www.wired.com/2014/10/verizons-perma-cookie/ (quoting EFF technologist Jacob Hoffman-Andrews); *see also* Mark Bergen & Alex Kantrowitz, *Verizon Looks to Target Its Mobile Subscribers with Ads* (May 21, 2014), http://adage.com/article/digital/verizon-target-mobile-subscribers-ads/293356/ (article from which Hoffman-Andrews learned of Verizon's technology).

[118] *See* Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, ELECTRONIC FRONTIER FOUND. (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

[119] *See id.* While website encryption would prevent Verizon from inserting the supercookie, it is the choice of the website provider and not the consumer whether to use encryption for any given web request, so a consumer could not "choose" encryption to avoid the supercookie.

[120] Jonathan Mayer, *How Verizon's Advertising Header Works*, WEB POL'Y (Oct. 24, 2014), http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/.

the practice of using supercookies to track its customers in 2012, Verizon did not provide any information on how its supercookie differed from standard tracking software (and that customers would still have trackable supercookies in their Internet traffic even if they opted out of the advertising program) until outside investigators discovered the supercookie in the fall of 2014.

What makes this a case study between FCC and FTC jurisdiction is Verizon's unconcern about its tracking practices when broadband was regulated as a Title I information service and policed by the FTC, in contrast to its swift compliance with FCC jurisdiction. Verizon did not promise to allow customers to opt out of supercookies entirely until February 2015, after the FCC Chairman Wheeler had begun to make clear that the FCC would not only to reclassify broadband as Title II, but also apply § 222 to broadband providers.[121] Verizon did not implement its opt out commitment until April 2015,[122] the month before the FCC's reclassification order (and with it application of § 222) went into effect.

Clearly, Verizon did not feel the same pressure to protect user privacy under the FTC's regime. This is not surprising. Given the vast range of businesses that the FTC must police, and the difficulty for the FTC to establish a violation of section 5 based on lax company handling of consumer data given the constraints of section 5(n) and the overall vagaries of the enforcement process, Verizon's decision to deploy supercookies on its more than 100 million wireless subscribers is easy to understand. Once subject to the laser-like focus of the FCC on broadband, and the clear FCC authority to enforce the privacy provisions of § 222, Verizon swiftly modified its behavior.[123]

---

[121]Verizon announced its new opt out policy on February 2, 2015. Mike Snider, *Verizon to Let Users Opt Out of "Super Cookie" Identifier*, USA TODAY, http://www.usatoday.com/story/tech/personal/2015/02/01/verizon-opt-out-supercookies/22697549/. Chairman Wheeler officially announced his proposal — including application of 47 U.S.C. § 222 — on February 4, 2015. Tom Wheeler, *FCC Chairman Tom Wheeler: This Is How We Will Ensure Net Neutrality*, Wired (Feb. 4, 2015), http://www.wired.com/2015/02/fcc-chairman-wheeler-net-neutrality/; Fact Sheet, *Chairman Wheeler Proposes New Rules for Protecting the Open Internet* (Feb. 4, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-331869A1.pdf.

[122]Rob Pegoraro, *How to Turn Off Verizon's 'Supercookie' Tracking*, USA Today (Apr. 5, 2015), http://www.usatoday.com/story/tech/personal/2015/04/05/verizon-supercookie/25247591.

[123]Also of note, AT&T wireless had engaged in a similar "experimental" tracking program, but had terminated its program in November 2014, just days after President Obama announced his support for FCC reclassification of Title II. *Compare* Statement on Internet Neutrality, Daily Comp. Pres. Doc. No. 841 (Nov. 10, 2014), *available at* https://www.gpo.

3. The FTC and FCC Are Structured So Differently Because They Have Complementary, Not Competing, Functions

To understand the difference between the FTC and the FCC, we need to understand the different institutional structures and different missions of the FCC and the FTC generally, not merely as part of the privacy debate.

The communication industry, for all its complication and differentiation, shares many common elements that lend itself to industry-wide oversight and industry-wide rulemaking. As Chairman Wheeler of the FCC has observed, networks generally have unique features that distinguish them from other industries.[124] Additionally, as Congress and the FCC have recognized, broadband and other telecommunications services are essential in our daily lives. As a consequence, Congress requires that the FCC regulate communications networks so that they affirmatively advance the public interest, convenience and necessity.[125]

In addition, while technically complex and differentiated from one another, all communications networks have certain elements in common. These include large upfront costs followed by very low marginal costs of adding subscribers, significant power from "network effects" (the more subscribers you have, the more valuable connection with your network becomes), and the capacity to operate as an intermediary between the subscriber and anyone trying to reach the subscriber (what economists refer to as a "two-sided market"). All of these contribute to factors that actively push communications markets to become highly concentrated.[126] Without regulatory oversight, communications markets easily slide into a "natural monopoly" or oligopoly, subjecting consumers to "take or leave it" terms that may include abusive access to consumers' most sensitive information.[127]

Finally, as noted above, because communications infrastructure is so critical to the security and economic well-being of the country, it requires a unique regulator capable of balancing these concerns and advancing federal policy to promote public safety and universal access. While the

---

gov/fdsys/pkg/DCPD-201400841/pdf/DCPD-201400841.pdf, *with* Elizabeth Weise, *AT&T Ends Tracking of Customers by "Supercookie"*, USA TODAY, http://www.usatoday.com/story/tech/2014/11/14/att-supercookies-tracking/19041911/.

[124] *See* TOM WHEELER, NET EFFECTS: THE PAST, PRESENT, AND FUTURE IMPACT OF OUR NETWORKS 20–21 (2013), *available at* https://transition.fcc.gov/net-effects-2013/NET_EFFECTS_The-Past-Present-and-Future-Impact-of-Our-Networks.pdf.

[125] *See* 47 U.S.C. §§ 214, 301.

[126] *See* WHEELER, *supra* note 124, at 23–24.

[127] *See id.* at 27.

FCC must protect consumers (and competitors) from the high potential for abusive information gathering practices, the FCC must also balance privacy protections against the needs of public safety and the need to promote investment and innovation by the network operators themselves.

By contrast, the FTC is organized on a theory of a generally functioning market and where enforcement action should be the exception, not the rule. It only acts when the market fails to adequately protect consumers because a business acts in an "unfair and deceptive manner," not because the industries it policies pose unique risks to consumers or have a general obligation to act in the public interest.

As a consequence of their very different missions, and very different designs, the agencies act in a complementary fashion. Arguments that this difference is somehow "bad" or "confusing" for consumers is rebutted by the 8 decades in which the FCC and FTC have maintained precisely this complementary relationship.

D. The FTC Has A Long History of Coordinating With The FCC, And Is Positioned To Do So In The Area of Privacy Protection

As noted above, the FTC and the FCC are hardly strangers to one another. Sine the Communications Act of 1934 brought the FCC into existence, the FTC and the FCC have cooperated to protect consumers and competition across the FTC's "Common Carrier Prohibition." A few case studies briefly illustrate this point.

Shared jurisdiction over merger review. The FCC has always reviewed the transfer of licenses by communications providers, broadcasters, cable operators, and wireless service providers generally.[128] In 1975, the Hart-Scott-Rodino Antitrust Improvements Act of 1976 required all proposed mergers above a certain dollar value to be reported to the Department of Justice (DoJ) and the FTC for potential review of antitrust concerns. [129] Although the FTC does not review mergers involving telecommunications, it has traditionally reviewed mergers involving cable and other non-telecommunications services with the FCC.[130]

[128] *See* §§ 214(a), 310(d).

[129] *See* Hart-Scott-Rodino Antitrust Improvements Act of 1976, Pub. L. No. 94-435, sec. 201, 90 Stat. 1383, *codified as amended at* 15 U.S.C. § 18a.

[130] Dissenting from the FTC's closing of the review of the proposed merger between Time Warner, Comcast, and Adelphia, two commissioners wrote:

Cooperation over the "Do Not Call" List. To address the increasing problem of aggressive telemarketing, Congress passed two complementary statutes. In 1991, Congress directed the FCC to regulate phone services and telecommunications technologies used for autodialing and robocalling consumers.[131] Congress supplemented this with passage of the the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994, which directs the FTC to regulate the practices of telemarketers to prohibit abusive telemarketing practices.[132]

This explicit complementary authority of the FTC and the FCC illustrates how both agencies bring their unique structure and expertise together to protect consumers. The FCC is charged with regulating matters under its expertise – the practices of communications networks and communications equipment. By contrast, the FTC is directed to regulate the practices of the telemarketing *businesses*, a matter well understood by the FTC but wholly foreign to the FCC.

But another way, Congress order the FCC to deal with the network and the FTC to deal with "edge providers." This collaboration has proven far more successful and beneficial to consumers than any misguided attempt to make either agency solely responsible for solving the entire problem of "telemarketing." Similarly, we can expect the FCC and the FTC to cooperate jointly to apply their expertise to protect consumer privacy with the FCC exercising jurisdiction over the network, and the FTC exercising jurisdiction over the edge providers.

> While we would have preferred that the Commission seek such relief, reasonable people can disagree (and do) about whether this acquisition is likely to harm consumers. And, in fact, another Commission, the FCC, continues to review this transaction under its more flexible "public interest" standard. . . . The role of this Commission does not have to end with our closing this investigation.

Statement from Jon Leibowitz & Pamela Jones Harbour, Comm'rs, Fed. Trade Comm'n, *Closing of the Investigation into Transactions Involving Comcast, Time Warner Cable and Adelphia Communications* 3 (Jan. 31, 2006), *available at* https://www.ftc.gov/public-statements/2006/01/statement-commissioner-jon-leibowitz-commissioner-harbour-concerning.

[131] *See* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, sec. 3(a), 105 STAT. 2394, *codified as amended at* 47 U.S.C. § 227.

[132] *See* Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994, Pub. L. No. 103-297, 108 STAT. 1545. In 2003, Congress supplemented this further with authorization for the FTC to maintain the national Do Not Call Registry. Act of Sept. 29, 2003, Pub. L. No. 108-82, 117 STAT. 1006.

General Memoranda of Understanding on Consumer Protection of Telephone Subscribers. Although the FTC is prohibited from applying section 5 to common carrier services, such as telephone subscriptions, both the FTC and the FCC have recognized that companies regulated as communications providers offer many non-communications services, subject to either joint FCC/FTC jurisdiction or FTC jurisdiction alone. For example, in 2000, the FTC and the FCC issued a joint policy statement on consumer protection in long-distance telephone services.[133] This joint policy statement has provided a basis for interagency cooperation for more than 15 years.

Particularly, the joint statement dealt with the practice of "slamming," a practice where consumers found themselves transferred from their long-distance provider of choice to an unauthorized long-distance carrier, usually being charged significant fees in the process. Again, the FCC directed itself to protecting consumers from the carriers over which it had jurisdiction, whereas the FTC protected consumers from third party "edge providers" engaged in unfair practices to deceive consumers to obtain consent (or to obtain information that allowed them to transfer and charge consumers without consent).

As part of the preparation for the FCC's enhanced jurisdiction in protecting the consumer from BIAS providers, the FCC and the FTC have entered into a similar Memorandum of Understanding.[134] Given the success over the last 15 years of the previous joint effort, there is every reason to believe that shared jurisdiction between the FCC and FTC will continue to enhance overall consumer protection.

E. The FTC has Similar Shared Jurisdiction With Other Agencies

Finally, it is worth noting in passing that this complementary jurisdiction between the FTC and other specialized agencies is hardly unique to the Federal Communications Commission. The FTC has complementary jurisdiction for consumer protection and privacy with other regulators of common carrier services, and other specialized agencies.

For example, although energy policy is ordinarily the domain of the Federal Energy Regulatory Commission,[135] the FTC does protect con-

[133] *In re* Joint FCC/FTC Policy Statement for the Adver. of Dial-Around & Other Long-Distance Servs. to Consumers, 15 F.C.C. Rcd. 8654 (2000).

[134] *See* FCC-FTC Memorandum of Understanding, *supra* note 75.

[135] *See* 42 U.S.C. § 7172 (FERC jurisdiction).

sumers by regulating the display of EnergyGuide labels to ensure that consumers make informed choices and protect consumers from fraudulent claims about energy efficiency.[136] The FTC and the FDA have joint jurisdiction of advertising and labeling of foods, drugs and cosmetics.[137] While the Department of Health and Human Services generally administers privacy of medical information, the FTC exercises complementary jurisdiction over those with access to personal medical information not covered by HIPAA.[138]

As this partial list demonstrates, not only is exercise of complementary jurisdiction nothing new to the FTC and the FCC, it is not particularly unique to the FCC either. Curiously, there is no concerted industry push to shift the entire burden of regulating health privacy, for example, or consumer protection in drug labeling, to the FTC. Only in the case of the FCC has this fairly common (and highly effective) regime been challenged. Yet there is no evidence to support any of the arguments advanced for stripping the FCC of its general consumer protection authority, or its specific privacy authority.

F. Conclusion: The FCC Should Take the Lead in Protecting Consumer Privacy and OTT Competitors from BIAS Providers

One would think that, if complementary jurisdiction between the FTC and the FCC were a problem, that evidence demonstrating the nature of this supposed problem would have emerged over the 80 years of complementary jurisdiction on consumer protection since passage of the Communications Act of 1934. If the problem were unique to complementary jurisdiction over privacy in particular, we would have expected some evidence to emerge in the more than 30 years that Congress expressly directed the FCC to protect cable subscriber privacy. At a minimum, there should be some highly documentable record of problems frustrating consumers since Congress directed the FCC to explicitly protect consumer privacy – and the privacy of OTT competitors and "edge providers" – since passage of the Telecommunications Act of 1996.

---

[136] *See* 16 C.F.R. §§ 305.11–.20.

[137] *See* Taylor & Feld, *supra* note 72, at 440.

[138] *See* Health Breach Notification Rule, 16 C.F.R. §§ 318.1–318.9; Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 17937 (providing FTC with authority over data breach notification for "vendors of personal health records and other non-HIPAA covered entities").

Opponents of the FCC following the Congressional direction have not produced any such record. Rather, their chief complaint appears to be that the FCC does *too* good a job protecting consumer privacy (and the proprietary information of competitors). They lament the "unfairness" that Google (as both a search engine and an operating system) can Facebook have greater freedom to collect consumer information. Phrased more politely, opponents to FCC action generally argue (a) whatever the FCC does doesn't matter, because other entities can similarly collect consumer information (and therefore, presumably, why bother?); (b) Somehow, FCC action on carriers under its authority distracts the FTC from acting to address broader privacy concerns.

If these arguments seem irrational, one should recall that the same carriers (and their same supporters) made similar arguments by non-sequitur in the first 5 years of the network neutrality debate. Apparently, preventing Comcast from blocking peer-to-peer applications or requiring Netflix to pay interconnection fees based on how popular it was as an OTT competitor was meaningless unless the FCC simultaneously ensured that Google did not favor its own products in its search engine. Similarly, it seems the ultimate triumph of the "corporations are people, my friend"[139] view to sacrifice the privacy of more than 100 million mobile subscribers in "fairness" to Verizon.

Fortunately, one need not appeal to the rules of logic or the questionable morality of violating the privacy rights of broadband subscribers to carriers as a matter of "fairness." As demonstrated in Part III, both the technology employed by broadband carriers, and their unique role in the broadband ecosystem, justify a different regulatory regime than for edge providers. The concerns that prompted Congress to enact § 222 in the Telecommunications Act of 1996 have increased, not diminished, with the changing world of telecommunications.

[139] Ashley Parker, *"Corporations Are People," Romney Tells Iowa Hecklers Angry Over His Tax Policy*, N.Y. Times, Aug. 12, 2011, at A16; *cf.* Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010).

Part III: The Serious but Correctable Threats to Privacy that Broadband Providers May Pose

The strong consumer privacy protections enabled by the FCC's CPNI authority can and should be used to vigorously protect broadband subscribers' information, because of the uniquely pervasive threat that BIAS providers pose to their consumers' privacy.

BIAS providers enjoy an unusually comprehensive view into their subscribers' lives, because they carry and thus can analyze the enormous quantities of Internet data that those subscribers transmit. Internet data is unusually rich in information, revealing information about a subscriber's habits, interests, political views, and more. And much of this information is sent unintentionally, due to advancing and connected technological devices of the Internet of Things as well as to simply the increasing essentiality of Internet services to citizenship and daily life.

Indeed, the practices in which BIAS providers *currently* engage reveal a frightening world of privacy-invasive activities. Faced with a lucrative market for selling off data of consumers, providers collect data ranging from search queries to sites visited, they inject tracking beacons into subscribers' data requests, and they even modify the web pages they deliver to include their own advertising. Such practices already greatly harm consumers' expectations of privacy and reliable communications service, and the broadening reach of the Internet will only exacerbate the bad incentives toward exploitation of subscriber data.

The privacy threat presented by BIAS providers far exceeds the concerns posed by edge providers such as search engines or social networking sites. Broadband providers uniquely enjoy a confluence of both a total view into subscribers' Internet access habits on the one hand, and knowledge of physical information about subscribers such as home address and financial information on the other. Edge providers generally have only one or the other of these, and importantly consumers always have the ability to opt out of giving any edge provider one or both of these compo-

nents of personal information. But consumers generally cannot opt out of a BIAS provider's data collection without opting out of the Internet entirely. This unusual monopoly power over consumer privacy, wielded only by BIAS providers, demands greater scrutiny—the sort of scrutiny authorized by the CPNI statute.

A. Broadband Providers Have Access to Vast Quantities of Valuable Personal Information

BIAS providers are especially concerning when it comes to consumer privacy, because they have access to enormous amounts of comprehensive and revealing information about their subscribers based on those subscribers' communications. That already large quantity of private information is only going to increase as technologies such as the Internet of Things advance. These unique concerns point to a need for a unique scheme of oversight over BIAS providers' use of that data, a scheme well-suited to the CPNI framework.

1. The Revealing Nature of Internet Communication Headers

To communicate on the Internet, a user identifies a service with which the user wants to interact, establishes a connection with that service, and exchanges data with that service in a series of information chunks called "packets." Each individual packet is much like a filled envelope, containing a "header" of addressing information indicating the packet's origin and destination locations, and a "payload" (also called the "body" or "content") of information to be delivered.[140]

Every packet that is sent to and from a subscriber must make its way through the subscriber's broadband provider. This means that the provider has access to an enormous quantity of information merely from this packet-based information exchange.

[140] This is a highly simplified explanation, though it is accurate for purposes of this paper. More specifically, data on the Internet is generally sent as a packet-within-a-packet. The payload is first enclosed according to the Transmission Control Protocol, which adds a header describing where an individual packet fits into a larger stream of data. *See* INFO. SCIS. INST., RFC 793, TRANSMISSION CONTROL PROTOCOL 3–5 (1981). That TCP packet is then itself used as a payload for a second layer of encapsulation, according to the Internet Protocol, which adds IP address information. *See* INFO. SCIS. INST., RFC 791, INTERNET PROTOCOL 11 (1981). Further layers of encapsulation, such as Ethernet frames, and alternate protocols such as UDP are beyond the scope of this discussion other than to note that they generally do not change the TCP/IP–based privacy analysis here. *See generally In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001).

The header of each packet contains three pieces of relevant information.[141] It includes the Internet Protocol (IP) address of the subscriber and the IP address of the service being accessed. The IP address of the service being accessed can indicate much information about the subscriber based on the nature of the service: a household of children, for example, is likely to visit Disney's website; a domestic violence victim far more likely to be accessing helpline information.[142] IP addresses can easily be mapped to geographic locations, meaning that both the subscriber and the service can be located.[143] While the geographic location of most Internet services would be uninteresting from a privacy perspective — everyone knows where Amazon is located — if the subscriber is using a peer-to-peer or direct-connection service such as Skype, the "service" may actually be another individual.[144] Thus, IP address information could potentially not only reveal the subscriber's location but also the locations of friends or relations.

The header also includes a port number, which the service will use to determine how to use the packet's data. A port number of 80, for example, is used for web page requests,[145] emails are sent using port number 25,[146] and Spotify uses port 4070 for peer-to-peer music distribution.[147] A subscriber's particular use of port numbers can thus reveal the types

[141] Again, this information is split between the TCP and IP encapsulation: the port number is in the TCP header, while the IP addresses are, unsurprisingly, in the IP header.

[142] *See, e.g.*, Tech. Analysis Branch, Office of the Privacy Comm'r of Can., What an IP Address Can Reveal About You (2013), https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf (noting wide range of information that may be discerned from an IP address).

[143] *See* Dan Jerker B. Svantenson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet"*, 23 J. Marshall J. Computer & Info. L. 101, 109–11 (2004).

[144] *Cf.* Brian Krebs, *Privacy 101: Skype Leaks Your Location*, Krebs on Security (Mar. 13, 2013), http://krebsonsecurity.com/2013/03/privacy-101-skype-leaks-your-location/.

[145] *See* J. Reynolds & J. Postel, RFC 1700, Assigned Numbers 19 (1994), https://www.ietf.org/rfc/rfc1700.txt.

[146] *See id.* at 16; Jonathan B. Postel, RFC 821, Simple Mail Transfer Protocol 44 (1982), https://www.ietf.org/rfc/rfc821.txt. Some Internet service providers already inspect subscriber data for port 25 traffic, primarily to block spam. *See* Chris Wilson, *What's "Port 25," and What Does It Have to Do with E-mail Spam?*, Slate Mag. (July 1, 2008), http://www.slate.com/articles/news_and_politics/explainer/2008/07/the_spam_superhighway.html.

[147] *See How Do I Configure My Router for Spotify?*, Spotify Support (last visited Feb. 12, 2016), https://support.spotify.com/us/problems/#!/article/how-do-i-configure-my-router-for-spotify.

of services that the subscriber uses, and thus potentially even the subscriber's interests or line of work. If a BIAS provider notices a subscriber frequently using port number 22, then the provider could infer that the subscriber is likely a computer software developer or system administrator, since traffic over port 22 generally relates to command-prompt logins to remote servers.[148]

Perhaps at an even more basic level, the time at which packets are sent can reveal yet more information about a subscriber. Researchers have found that timing of information can be so revealing that a person's password can be decoded merely by analyzing the times of keystrokes.[149] Timing can reveal the hours when a subscriber is awake, asleep, or at work. It can reveal a person's religious beliefs, as with observance of the Sabbath. It can reveal unexpected changes in lifestyle, such as holidays, new relationships, or lost jobs. Indeed, time of activity can be a matter of great personal privacy, such as when Justice Scalia contemplated "at what hour each night the lady of the house takes her daily sauna and bath — a detail that many would consider 'intimate.' "[150]

2. Deep Packet Inspection

As revealing as the packet headers may be, the payloads potentially reveal far more information. Although a BIAS provider only needs to inspect the header information for purposes of getting packets to their destinations, nothing stops the provider from reading the payload of any packet, unless the contents are encrypted — a practice that is the choice of the service being accessed, not the subscriber, and a practice that is used for less than 30% of Internet traffic today.[151] Unencrypted packets are like mail in a clear envelope: the carrier, in this case the BIAS provider, is able to read and understand them in their entirety.

---

[148]Specifically, port 22 is used for the Secure Shell (SSH) protocol. *See* T. YLONEN & C. LONVICK, RFC 4253, THE SECURE SHELL (SSH) TRANSPORT LAYER PROTOCOL 4 (2006), https://www.ietf.org/rfc/rfc4253.txt.

[149]*See* Dawn Xiaodong Song et al., *Timing Analysis of Keystrokes and Timing Attacks on SSH*, 10 PROC. CONF. ON USENIX SECURITY SYMP. No. 25 (2001), *available at* https://www.usenix.org/legacy/events/sec01/full_papers/song/song.pdf.

[150]Kyllo v. United States, 533 U.S. 27, 38 (2001).

[151]*See* SANDVINE INTELLIGENT BROADBAND NETWORKS, GLOBAL INTERNET PHENOMENA SPOTLIGHT: ENCRYPTED INTERNET TRAFFIC 3 & fig.1 (2015), https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf. Indeed, that number is skewed large, because much of the encrypted traffic volume is from the video site YouTube. *See id.* at 4.

The practice of Internet intermediaries gratuitously analyzing the payload of Internet packets is called "deep packet inspection,"[152] and it raises some of the greatest concerns for online privacy. Using deep packet inspection, a BIAS provider could theoretically put together every web request, email, voice-over-IP call, and other communication in which a subscriber participates, revealing a wealth of information about that subscriber.

Indeed, when the Federal Trade Commission considered the practice of deep packet inspection (abbreviated as "DPI"), it observed commenters who "cited the ability of ISPs to use DPI to monitor and track consumers' movements across the Internet." The FTC specifically noted that Internet service providers have "access to vast amounts of unencrypted data that their customers send or receive over the ISP's network," putting them "in a position to develop highly detailed and comprehensive profiles of their customers — and to do so in a manner that may be completely invisible."[153] This potential for privacy invasion led the Commission to have "strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection."[154]

3. The Increasing Pace of Data Generation, Creating Increased Opportunity for Privacy Violations

While no single piece of information described above may necessarily be greatly invasive of an individual's privacy, the sum total quickly approaches a zone of grave concern. In 2012, IBM estimated that 250 million gigabytes of information were generated on the Internet every day.[155] That massive quantity of data has led to an umbrella of data analysis and mining practices colloquially termed "Big Data," and it has opened the door to revelations of private information in truly unexpected ways.

For example, even when anonymized by stripping out personally identifying information, data can nevertheless reveal the identity of individuals through an analytic process called "deanonymization."[156] A 2012 in-

[152] *See, e.g.*, Thomas Margoni & Mark Perry, *Deep Pockets, Packets, and Harbors*, 74 Ohio St. L.J. 1195, 1199–201 (2013).

[153] FTC 2012 Privacy Report, *supra* note 91, at 56.

[154] *Id.* at 40, 56.

[155] Matthew Wall, *Big Data: Are You Ready for Blast-off?*, BBC News (Mar. 4, 2014), http://www.bbc.com/news/business-26383058.

[156] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716–22 (2010), http://www.uclalawreview.org/

vestigation revealed that the big-box chain Target, through aggregation of personal data, was able to determine whether young women were pregnant — at times even before they or their parents knew.[157]

And the potential for revealing data only increases as Internet of Things devices become more prevalent. Such devices install within a person's household numerous small computers in thermostats, refrigerators, door locks, and other devices. Many of these small computers communicate on the Internet, oftentimes without knowledge or consent of their owners. Those communications are often not encrypted due to the limitations of the devices.[158]

Internet of Things devices thus provide BIAS providers a new opportunity to collect a valuable category of data. The providers are in position not only to learn what devices the subscriber owns but also all information that those devices are reporting on their owners. Because the online activities of these devices are not always known to their owners, the BIAS provider, indeed, could easily know more information about subscribers than the subscribers ever believed they had revealed.

Accordingly, the volume of information passed from a subscriber through a BIAS provider provides an enormous opportunity for data collection of private information. No wonder, then, that a leading scholar described such providers as being "the single greatest point of control and surveillance."[159] These possibilities should raise significant concerns and

---

pdf/57-6-3.pdf (describing several examples of anonymized datasets where individual records were reidentified with individuals); Petition for Declaratory Ruling at 6–8, *In re* Petition of Pub. Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecomms. Providers without Customers Consent Violates Section 222 of the Commc'ns Act, WC Docket No. 13-306 (FCC Dec. 11, 2013).

[157] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html ("As [Target's researcher Andrew] Pole's computers crawled through the data, he was able to identify about 25 products that, when analyzed together, allowed him to assign each shopper a 'pregnancy prediction' score. More important, he could also estimate her due date to within a small window, so Target could send coupons timed to very specific stages of her pregnancy.").

[158] *See* Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016), https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/ (noting several Internet of Things devices transmitting video, ZIP codes, and other sensitive data without encryption); Lorenzo Franceschi-Bicchierai, *Nest Thermostat Leaked Zip Codes Over the Internet*, VICE: MOTHERBOARD (Jan. 20, 2016), http://motherboard.vice.com/read/nest-thermostat-leaked-home-locations-over-the-internet ("Some smart devices have such little computing power that they couldn't perform the necessary encryption processes even if their creators wanted them to . . . .").

[159] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1423.

highlight the need for close attention to how to oversee BIAS providers' use of this wealth of consumer information.

B. Current Anticompetitive Behavior

Online advertising is lucrative, and for a company with direct access to all of its users' browsing habits, it is also low-hanging fruit. Mobile advertising expenditures alone will likely crest $100 billion in 2016, while still only comprising *half* of the total digital advertising market.[160] Meanwhile, mobile broadband is experiencing an industry-wide slowdown, with analysts predicting a drop in growth rate from 4% to 3.1% in 2016.[161] ISPs are rapidly reaching a point where "traditional avenues for increasing revenue — voice, messaging and data — won't cut it."[162]

Companies have realized the proverbial cash cow in their pasture, and have begun to milk it. AT&T's CPNI-based advertising generates over $800 million in revenue annually — a total they insist would be irretrievably lost under rudimentary CPNI protections.[163]

In 2014, Verizon sought to capitalize on its users data by use of a "super cookie" — a unique tracking ID into each of its customers' traffic, which allowed the company to monitor its users' mobile browsing behavior in excruciating detail. The result was a security nightmare: the system handed the user's unique ID to every site she visited,[164] and some versions of the header contained unencrypted, highly private information, such as the user's phone number.[165] Despite substantial backlash, Verizon doubled down on its advertising ambitions and acquired former internet titan AOL for $4.4 billion last year. AOL's robust advertising presence allowed

[160]Lara O'Reilly, *Fresh from being bought by Verizon, AOL is reportedly preparing to acquire mobile ad tech company Millennial Media for $300 million*, Bus. Insider (July 9, 2015), http://www.businessinsider.com/report-aol-to-buy-millennial-media-for-300-million-2015-7.

[161]GSM Ass'n, The Mobile Economy 2015 (2015), http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf.

[162]Kevin Fitchard, *The Real Reason Verizon Bought AOL*, Fortune (June 24, 2015), http://fortune.com/2015/06/24/verizon-gains-aol/.

[163]Joint Petition for Stay of United States Telecom Association et al. at Exh. 9, para. 20, *In re* Protecting & Promoting the Open Internet, 30 F.C.C.R. 4681 (May 1, 2015) (No. 14-28), *available at* http://apps.fcc.gov/ecfs/document/view?id=60001046171.

[164]Stephanie Mlot, *Verizon to Share 'Super Cookie' Data with AOL's Ad Network*, PCMag (Oct. 7, 2015), http://www.pcmag.com/article2/0,2817,2492705,00.asp.

[165]Nader Ammari et al., The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy (2015), https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf.

Verizon to "expand beyond the telecom industry's limitations by using its extensive network to enter an entirely different industry."[166]

Though dogged, Verizon is not an anomaly. ISPs have already shown how hungry they are for CPNI — and how they want to use it. AT&T recently rolled out a "pay-for-privacy" offering, which adds a $30 per month premium to users who don't want their data tracked.[167] The "discount" offering tracks every aspect of a user's behavior, from search terms entered to links clicked and sites visited. The tracking cannot be turned off by normal means short of using a VPN, enduring even if users "clear cookies, use an ad block program, or switch on a browser's do-not-track settings."[168] The data goes directly to advertisers, allowing them to target ads and email directly to the user.[169]

Nor are ISPs shy about rerouting user traffic for their own benefit. A blogger discovered in 2013 that Comcast was hijacking his http requests to show him a data cap warning.[170] Comcast has also injected javascript ads for its own apps and services into websites without permission from the operators or users, creating potentially enormous security risks to both.[171]

C. Broadband Providers Pose a Greater Threat to Consumer Privacy Than Edge Providers

It is obviously not the case that BIAS providers are the only ones in a position to collect private data; edge providers, such as search engines, social networks, and e-commerce sites, have access to consumer information as well. But there is good reason to be more greatly concerned about BIAS providers' use of subscriber information, beyond the baseline privacy concerns that are commonly expressed about edge providers. This is because a subscriber will necessarily offer more comprehensive data to a

[166]Fitchard, *supra* note 162.

[167]*See* Stacey Higginbotham, *ISPs Really, Really Want to Be Able to Share Your Data*, FORTUNE (Apr. 28, 2015), http://fortune.com/2015/04/28/isps-share-your-data/.

[168]Elizabeth Dwoskin & Thomas Gryta, *AT&T Tacks a Privacy Charge on High Speed*, WALL ST. J. (Feb. 18, 2015), http://www.wsj.com/articles/at-t-tacks-a-privacy-charge-on-high-speed-1424314904.

[169]*Id.*

[170]Ryan Kearney, *Comcast Caught Hijacking Web Traffic*, RYAN KEARNEY (Jan. 9, 2013), http://blog.ryankearney.com/2013/01/comcast-caught-intercepting-and-altering-your-web-traffic/.

[171]David Kravets, *Comcast Wi-Fi Serving Self-Promotional Ads via JavaScript Injection*, ARS TECHNICA (Sept. 8, 2014), http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/.

BIAS provider than to any individual edge service, and the consumer has no meaningful ability to opt out.

1. More Subscriber Data, and No Way to Opt Out

Although edge providers are often criticized for their data collection practices, their practices are necessarily limited by the simple fact that consumers use many of them. The visits a user makes to one website will not automatically be known to other websites. Indeed, edge providers invest heavily in workaround services to attempt to track users across multiple sites — services that are highly imperfect and often relatively easily circumvented. The scope of information available to any edge provider is inherently limited.

By contrast, the BIAS provider has an almost panoptic view into its subscribers' Internet usage. Because households generally only have a single broadband connection, all Internet data must be sent over that single connection.[172] Indeed, even counting wireless devices, most households have at most two or three routes to accessing the Internet at all. This means that the BIAS provider already has a near-complete picture of any household's Internet activity, and a totally complete picture would only require data sharing agreements with the small number of wireless carriers on the market.

As one commentator drew the comparison between an ISP and perhaps the most well-known edge provider:

> Google cannot dream of building the same type of digital dossier that an ISP can, unless a user chooses to use Google for everything he does online. Google cannot know what users buy on Amazon or eBay, what they read on the *New York Times*, or who they friend on Facebook. An ISP can. Furthermore, Google can never know what a user does or says when he uses non-web Internet applications such as instant messaging or VoIP telephony. An ISP can.[173]

[172]Among households that have 25Mbps/3Mbps broadband service, 33% have access to two or more broadband provider options, and only 13% of those in rural areas have such multiple options. *In re* Deployment of Advanced Telecomms. Capability to All Americans in a Reasonable & Timely Fashion, GN Docket No. 15-191, ¶ 86, tbl.6 (Jan. 29, 2016) (2016 Broadband Progress Report).

[173]Ohm, *supra* note 159, at 1442.

And BIAS providers are at little disadvantage relative to edge providers in their ability to use that data. Unless the data is encrypted — the majority on the Internet is not — it is plainly readable to and usable by the BIAS provider in the same way it is to the edge provider. And even encrypted traffic still reveals a great deal of useful information in the packet metadata and timing of requests, as described earlier. But while edge providers can only mine the data they receive or contract for, the BIAS provider can mine a subscriber's usage of all websites, emails, and other Internet services. Quite in contrast to edge providers who must make arrangements with innumerable and unknown other services to even crack the surface of an individual's Internet usage profile, the BIAS provider has all the information it could want, delivered to it on a silver platter, day in and day out.

Furthermore, BIAS providers differ from edge providers in the ability of users to opt out of data collection. With edge providers, users have numerous self-help remedies to protect their privacy. For one thing, they can simply choose an alternative service; there is sufficient competition among most Internet services to allow users to select services most suitable to their privacy and other interests. Furthermore, users can adjust their browsing habits to avoid tracking by edge providers in many circumstances. They can delete browser cookies, for example, to remove tracking information, or install privacy-enhancing web filters to avoid sending data to third-party tracking services.[174]

These consumer options do not exist with respect to BIAS providers. The Verizon supercookie, for example, was widely noted for the fact that consumers could not opt out of it, even if they disabled cookie tracking entirely.[175] And because most households have only one available broadband connection, subscribers do not enjoy a choice among services; to opt out of a BIAS provider's data collection and sharing policies requires opting out of the Internet itself.[176]

---

[174] *See, e.g.*, Jennifer Valentino-DeVries, *How to Avoid the Prying Eyes*, WALL ST. J. (July 30, 2010), http://www.wsj.com/articles/SB10001424052748703467304575383203092034876.

[175] *See* Natasha Singer & Brian X. Chen, *Use of Mobile "Supercookies" Is Seen as a Threat to Privacy*, N.Y. TIMES, Jan. 25, 2015, at B2.

[176] That AT&T offered a pay-for-privacy option only highlights the degree to which subscribers are forced into their BIAS provider's data privacy policy. AT&T could offer that option or not, and it could charge whatever it wanted for that option; it does not face the competitive pressures to offer enhanced customer value in the form of better privacy protection in the same way that edge providers do.

2. Access to Sensitive Physical Information

Only enhancing the degree to which BIAS providers have the edge over edge providers in data collection capabilities is the amount of personal, physical information that BIAS providers maintain on their subscribers. Most providers require prospective subscribers to provide highly private information about themselves, most particularly social security numbers.[177] Those social security numbers are then generally used for credit checks, revealing to BIAS providers a great deal of financial information about their applicants.[178] Of course, providers also know the physical address, billing information, and other demographic information of their subscribers.

Few edge providers enjoy that level of detailed information into the actual lives of their users. A search engine, for example, does not require its users to enter financial information before conducting web searches. Edge providers that do receive such personal information are generally more specialized services, such as e-commerce sites or financial companies, with whom users would interact on a much less frequent basis. Thus, while some edge providers (such as search engines) may have a broad view of a subscriber's online activities and others (such as online banks) may have detailed personal information, few will have both of these. BIAS providers, on the other hand, will always have both.

3. A Problem for Competition

The ability to gather this kind of specific, textured information gives ISPs a substantial advantage over competitors when marketing their own affiliated products — even without deep packet inspection. As described above, timing and IP address information, which are not subject to encryption, are greatly revealing of much information about a subscriber's behaviors, interests, and so on. This information alone could potentially reveal if a person is unemployed (browsing a home connection during business hours, frequent visits to IPs associated with job hunting sites); raising children (business hours browsing of parenting sites); experiencing domestic violence (IPs associated with victim resources); seeking help for

[177] *See, e.g.*, Ed Bott, *Why Does Comcast Need My Social Security Number?*, Ed Bott (June 29, 2005), http://www.edbott.com/weblog/2005/06/why-does-comcast-need-my-social-security-number/.

[178] *See* Gerri Detweiler, *Will Bad Credit Stop You From Getting Cable?*, Credit.com (Mar. 24, 2014), http://blog.credit.com/2014/03/will-bad-credit-stop-you-from-getting-cable-78764/.

highly personal medical conditions (such as IP addresses for gender reassignment surgery providers); undergoing a divorce (divorce attorney domains); filing for bankruptcy; or any number of personal issues.

All of this amounts to an enormously valuable commodity for ISPs — both in marketing their own products and in selling the data to other networks. Frequent visits to IP addresses associated with home alarm companies can indicate to an ISP that their customer is shopping for a new alarm system. Frequent data exchanges to one of those IP addresses can reliably indicate a livechat with customer service. For an ISP who also owns a home alarm company (such as AT&T), this can be invaluable data, allowing them to offer their services before competitors are even aware that a potential customer is seeking them out. Such broad and deep data is also a massive asset to advertisers, both ISP-affiliated and independent. With a lucrative revenue stream at their fingertips, it would be more surprising if ISPs did not attempt to monetize the data by selling it to outside parties.

This striking advantage of BIAS providers in access to consumer data suggests a need for closer scrutiny and regulation of their collection and use of that data. The oversight of edge providers' data privacy practices is not sufficient. That oversight has often focused on data brokers who aggregate information among different services, for example. But a focus on data brokers might be misplaced when it comes to BIAS providers, since the providers, having so much data already at their fingertips, would likely be less dependent on data brokers. A specific solution, tailored to the particular privacy problems that BIAS providers pose, is necessary to properly protect the public.

Part IV: Recommendations for a General FCC Approach on Privacy Protection and BIAS Providers

As discussed at length above, the legal and historic foundation of the FCC's privacy protection jurisdiction, combined with the complementary role of the FTC, creates the fundamental framework and tool kit for the FCC to do the job Congress directed it to do. The catalog of actual and potential information gathering practices of BIAS providers, discussed in Part III[179] and addressed by others,[180] demonstrates an urgent and immediate need for the FCC to lay down ground rules now — before industry practices inimical to consumer privacy protection become firmly established industry norms.

A. The FCC's Role in Protecting Consumer Privacy, While Vitality Important, Is Narrowly Constrained

Of equal importance to recognizing what the FCC *should* do is recognizing what the FCC *should not* do. The FCC's jurisdiction over BIAS providers and other communications services (such as cable) derives from the unique role these communications services play in our economy, in public safety ad national security, and in that most fundamental of human activities — social interaction. The threats to consumers from commercial data trackers and government surveillance outside the narrow world of networks over which BIAS, voice service, and video travel are equally urgent and deserve immediate attention from Congress, the FTC and other relevant agencies. But the FCC should not — indeed must not — overstep its competency and Congressional authority by trying to solve the entire complex problem on its own.

[179] *See* Part III *supra* p. 45.

[180] *See, e.g.,* Open Tech. Inst., New Am. Found., The FCC's Role in Protecting Online Privacy (2016), https://www.newamerica.org/oti/the-fccs-role-in-protecting-online-privacy/.

Rather, the FCC's role in protecting consumer privacy online is limited by its area of institutional competence and statutory authority. Through its cooperative relationship with the FTC it works to clarify and simplify the issues the FTC must address. Where Google or Facebook offer telecommunications services, then the FCC regulates them as communications providers to the extent they offer such services.[181] Similarly, while the FCC regulates Verizon's telecommunications services, it does not regulate Verizon's advertising business.

In the world of convergence, there may well be gray lines and hybrid services, as there were in the world of voice service 20 years ago. Certainly the Commission should monitor and carefully consider whether services that began life as "information services" have evolved into telecommunications services. But the Commission should always proceed mindful of the limitations of its expertise and authority.

B. How the FCC Should Triage Issues and Adopt Rules

The Open Technology Institute of the New America Foundation (OTI) recently published a white paper on what rules the FCC should adopt to protect online privacy.[182] These proposals include a broad definition of CPNI, clear and full disclosure of how BIAS providers intend to use any information collected, a requirement that consumers must affirmatively "opt in" to any sharing of their information, and a simple, straightforward complaint process for consumers to use.

All of these are important specific proposals and the FCC should certainly move swiftly to implement them. In addition, as discussed below, the FCC must explore how to ensure that customers are not charged a premium to protect their statutory right to privacy, while honoring Congressional intent to give consumers full control over their information.

But more important than any specific proposal is the method by which the FCC should analyze the complex issues raised by the evolution of broadband telecommunications services and develop a consistent approach that protects consumers, promotes competition, and is consistent with the functional operation of the Internet. This analysis must consider the increasing bundling of broadband with cable video services (governed by the cable competition and privacy provisions of the Communications Act) and mobile services (regulated under Title III of the Act). This

[181]But, in the words of 47 U.S.C. § 153(51), each would be a telecommunications carrier "only to the extent that it is engaged in providing telecommunications services."

[182]*See id.*

bundling of services raises the same competition issues that they raised in the traditional telephone world in the 1980s, which prompted the FCC to invent the concept of CPNI in the first place. This historic experience, combined with the expertise contributed by the FTC and the examination of existing broadband capabilities and practices, provides a suitable framework for considerations.

1. Consent To Reveal CPNI Does Not Include Consent To Reveal Content

Even when telephone subscribers allowed their phone company to access their CPNI, the phone company never actually listened to the content of the call. A phone company could know if a person received a call from the local pharmacy, but the company could not listen to the content of the call to know that it was to pick up a prescription for AIDS medication or birth control pills.

Additionally, broadband, like telephone service, is a two-way connection. An initiator of a call or Internet request has no way to know if the recipient is or is not permitting a provider to view the content of the initiator's communications.

Nevertheless, as discussed above, broadband providers can use technologies like deep packet inspection (DPI) to access not merely traditional types of CPNI, but the actual content of information. As the FTC recognized in its 2012 Privacy Report, DPI in particular raises grave privacy concerns because it potentially reveals such a vast amout of highly sensitive information, so that even consumers who do consent may not be able to appreciate the scope of information revealed.[183]

Accordingly, the Commission should prohibit *any* provider under *any* circumstances from using DPI or other tools to view the content of subscriber traffic. A consumer cannot consent to have information prohibited under § 222(b) to become usable to BIAS providers because the consumer consents to intrusive surveillance such as DPI. Nor can one broadband subscriber consent to have the information of another broadband provider revealed via DPI or other means, since the sending subscriber has no way of knowing if the receiving subscriber has consented to such intrusive content scanning or not.[184]

---

[183] *See* FTC 2012 Privacy Report, *supra* note 91, at 56. *See generally* Section III.A.2 *supra* p. 48.

[184] Pursuant to the exceptions in 47 U.S.C. § 222(c), the prohibition on carriers reading the content of a subscriber's communications will not interfere with the legitimate needs

2. The FCC Should Restate Its 2007 Holding that CPNI Includes Personal Private Information, and Its Framework for Assessing the Level of Privacy Protection

In 2007, the FCC explicitly held that "CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services."[185] The 2007 Order meticulously laid out the general framework of how the FCC analyzed the "general duty of all carriers" to protect CPNI, including enhanced concern over the greater need to protect personal information that has the potential to cause economic loss or other harm to customers.[186] The FCC explicitly rejected a proposed "safe harbor" rule because: "The public interest is better served if the Commission retains the option of taking strong enforcement measures regarding carriers' duties under Section 222 and the Commission's rules."[187] The FCC established a rebuttable presumption that if a breach occurred, it occurred because the carrier had failed to take adequate precautions and therefore failed under its general obligation to protect customer information under § 222(a).[188]

Finally, the FCC advised carriers that as new precautions became necessary, carriers would be obligated, *of their own accord and without the need for any additional rulemaking*, to increase their level of protection for customer information under the general duty imposed by § 222(a): "Of course, we require carriers to implement the specific minimum requirements set forth in the Commission's rules. We further expect carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier."[189]

The 2007 Order setting forth the FCC's authority and general approach to CPNI would seem to resolve the vast majority of objections and concerns raised recently by carriers.[190] The FCC should therefore begin by re-

---

of law enforcement or the ability of BIAS providers to maintain their networks or collect aggregate information.

[185] *In re* Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927, ¶ 1, n.2 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking), *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009).

[186] *Id.* ¶¶ 37–50.

[187] *Id.* ¶ 66.

[188] *Id.* ¶ 63.

[189] *Id.*

[190] Some such citations were raised in Petition for Partial Reconsideration of CTIA — The Wireless Association, *In re* Lifeline & Link Up Reform & Modernization, Telecomms. Carriers Eligible for Universal Serv. Support, Connect Am. Fund, 30 F.C.C. Rcd. 7818 (Aug.

stating the framework and interpretation of its authority it unanimously adopted in 2007. The broad definition of CPNI and the unwavering commitment to protecting consumer privacy the FCC are as necessary a foundation for privacy online as they were for traditional voice service.

3. The FCC Should Prohibit BIAS Providers from Interfering with a Subscriber's Use of Privacy Enhancing Tools that Customers Are Accustomed to Using when Browsing, and Require BIAS Providers to Protect Personal Information from Third Parties

Consumers at the moment have a number of options for clearing tracking software when they go online that are short of encryption or virtual private networks (VPNs), but suffice for some purposes under the codes of conduct established by edge providers and monitored by the FTC. For example, browsers permit customers to "clear cookies" or other tracking software. The reason the Verizon tracking identification system was termed a "supercookie" was because — while customers could still shield themselves with encryption and the use of VPNs — these standard practices that consumers can easily and predictably use did not work to eliminate the tracking code.

The Commission should prohibit carriers from using tracking methods that defeat customer efforts to enhance their privacy, or that expose their information to third parties. This includes not merely a prohibition on breaking encryption or VPNs, but on methods such as browser clearing. At a minimum, the Commission must require that any such methods require explicit notification that traditional methods of avoiding tracking such as browser cache clearing will not prevent tracking by the BIAS provider.

This raises an additional concern. Privacy is not a simple on/off matter, where consumers must expose everything or nothing. A consumer may expect to expose certain information to Facebook or Google, for example, in exchange for free services. But if a consumer wants to avoid tracking for a particular communication or transaction, the consumer can take measures like blocking application access to data or clearing a browser cache of tracking software.

The Commission should explore how to avoid BIAS providers from converting consent to the use of certain information for certain purposes into general consent for all purposes. At a minimum, the Commission

13, 2015) (WC Docket Nos. 11-42, 09-197, 10-90), *available at* http://apps.fcc.gov/ecfs/document/view?id=60001121721.

must permit consumers to change their minds with regard to allowing or denying the BIAS provider access to information in the same way that consumers expect to be able to enable or disable access to information by applications.

4. The Burden to Protect Private Information Lies with the Carrier, Not the Consumer

Unlike applications, however, BIAS providers may not deny consumers the full value of their broadband connection unless consumers "consent" to BIAS use of their information. Section 222 places the burden of privacy firmly on the telecommunications service provider, not on the customer. Suggestions that consumers bear the responsibility to protect their own privacy through encryption or VPNs, that BIAS providers may charge additional fees for privacy, or that BIAS providers can withhold critical functions or services to coerce user consent, should therefore be swiftly and forcibly rejected by the FCC.

In § 222, as well as in section 631,[191] Congress made it crystal clear that intended consumer privacy to be a statutory *right*, not a privilege. Section 222(a) establishes the general duty on all carriers to protect all customer proprietary information. The statute is utterly devoid of *any* statutory language that remotely suggests any "balancing" in harms between consumers and carriers. To the contrary, the legislative history makes clear that Congress intended to place the responsibility, and therefore the burden, firmly on carrier.

This authority is not, of course, unlimited. The burdens that the Commission places on a carrier must be justified by the administrative record[192] and remain cognizant of the requirement to avoid restrictions which would prevent the carrier from providing the telecommunications service. Nevertheless, it is important to stress that FCC's jurisdiction in this regard is profoundly different from that of the FTC's under section 5 of the FTCA. As discussed above, section 5(n) requires the FTC to consider, among other things, whether the consumer could have taken mea-

[191] Cable Communications Policy Act of 1984 § 631, 47 U.S.C. § 551.

[192] *See, e.g.*, U.S.W., Inc. v. FCC, 182 F.3d 1224, 1234 (10th Cir. 1999) ("When faced with a constitutional challenge, the government bears the responsibility of building a record adequate to clearly articulate and justify the state interest.").

sures to avoid the injury. Section 222 is not merely devoid of any such consideration; it explicitly rejects such an approach.[193]

This bears particular emphasis in light of recent suggestions that the Commission could forgo rules and enforcement under § 222 since subscribers have access to encryption and VPNs.[194] While carriers should be prohibited from interfering with these privacy enhancing tools, their availability to consumers does not allow carriers to shift the cost of privacy to consumers, or in any way mitigate the carrier responsibility to protect consumer privacy under § 222. Consumers, particularly the poor, should not be required to pay an additional monthly fee, over and above the already costly price of a broadband subscription to subscribe to a VPN service. Nor should they be required to obtain the technical proficiency to use encryption. Congress did not intend to convert the right of privacy into a luxury good available only to those who can afford it, nor does § 222 allow the FCC to adopt such an approach.

Prohibit BIAS providers from coercing consent by charging fees or withholding functionality. In the general marketplace for applications and online services, it is considered acceptable to demand access to consumer information both to ensure functionality and as part of the "payment" for the service. For an essential service such as broadband access, however, Congress made a deliberate choice to prohibit such practices. Communication, including broadband communication, is an essential service. There is a significant and dramatic difference between access to a basic service essential to participating in modern society and deciding whether or not to download an application that mimics a compass or a level.

Congress clearly could tell the difference, as demonstrated by the decision to put essential communication services under § 222 and to leave applications that mimic tools to the FTC under section 5. The FCC should not permit endless hand waving demanding a "level playing field" to obscure the rather large difference between access to the Internet and the decision to download a convenient tool.

Accordingly, the FCC must prevent BIAS providers from coercing consumer "consent" from a user by withholding service, or in any way disabling services that a subscriber reasonably assumes are included as part

[193]The protections of 47 U.S.C. § 222 are automatic, regardless of whether a consumer acts to invoke them.

[194]*See, e.g.,* Richard Bennett, *Bringing Privacy into the Open*, High Tech F. (Jan. 26, 2016),//hightechforum.org/bringing-privacy-into-the-open/.

of the purchase of a Title II broadband service. Nor should the FCC permit BIAS providers to charge for privacy protection under the guise of "administrative privacy fees" or "premium" services.

5. Inducements To Consent, Such As Service Discounts, Require Careful Scrutiny

This, of course, raises the question of BIAS providers offering financial discounts and other inducements to consent to allow access to CPNI, sometimes referred to as "pay for privacy." For example, as discussed above, AT&T has offered a discount to customers of its "Gigapower" gigabit service if they will permit AT&T to track their online information.[195]

As noted above, the Commission should prohibit such "discounts" or "incentives" when they are, in fact, coercive tools to force consumers to give up their statutory rights. At the same time, however, Congress clearly intended that consumers should have control of their own information. Additionally, even where discounts and incentives are genuine, the Commission must consider the concerns noted above with regard to its obligation to protect proprietary information belonging to competitors reaching their customer through the BIAS provider, and protecting the privacy of consumers who have not consented to have their personal information collected as the cost of contacting the subscriber who has opted in to the collection of personal information.

Finally, the Commission must consider the social implications inherent in disclosing privacy in exchange for essential services. On the one hand, a provider offering a genuine discount clearly recognizes the value of the information, and reasonably offers to compensate the consumer. If this allows poorer people to have access to higher speeds than they might otherwise be able to afford, should this practice be permitted? On the other hand, because it is difficult to police whether the promised discounts are a result of deliberately inflated prices to coerce customers to permit tracking their online behavior, and because the poor are most vulnerable to this form of coercion, should the Commission ban the practice as inherently unjust and unreasonable?

In exploring this issue, the Commission should consider that it is not an either or decision. The virtue of the Commission's rulemaking authority and waiver process is that it allows the Commission to make nuanced decisions based on specific circumstances, in addition to adopting broader general rules.

[195] *See* Higginbotham, *supra* note 167. *See generally supra* p. 52.

6. The Commission Should Explicitly Seek Comment on Enhancing Cable Privacy Rules Under Section 631 and Wireless Privacy Pursuant to Section 303(b)

The vast majority of broadband providers in the United States provide bundled services. These bundles generally include video programming, governed under Title VI of the Act, or wireless service offered by holders of exclusive licenses subject to Title III of the Act.

Providers such as Comcast, Verizon and AT&T have aggressively bundled their broadband services with their mobile and/or video service, raising questions as to the extent to which information regarding these services are intermingled by the companies and whether the carriers are using customer information collected through a cable service or mobile wireless service in combination with broadband services in ways not disclosed to customers. For example, it is reported that Comcast is exploring ways to monetize consumer information collected from its broadband and cable systems to advertisers to create highly personalized interactive advertisements.[196]

Cablevision already harnesses information from its cable service, broadband service, and VOIP service to individually market services to customers in precisely the way § 222 is designed to avoid, but which may or be not be permissible under section 631 of the CCPA in the absence of any specific rules from the FCC. At an investor conference in December 2015, Cablevision's President of Media Sales explained how Cablevision combines information from its cable service and broadband service to develop marketing information, which it then sells to third parties and uses for its own internal marketing purposes. According to one trade article describing the event:

> "We don't report it publicly, but over the last 18 months, [serving national advertisers with addressable data from set-tops] has grown to be pretty big part of our data business," said Ben Tatta, president of Cablevision Media Sales. "We're now able to offer advertisers much more granular measure-

[196] *See* Shalini Ramachandran and Suzanne Vranica, *Comcast Seeks to Harness Trove of TV Data*, Wall St. J. (Oct. 20, 2015), http://www.wsj.com/articles/comcast-seeks-to-harness-trove-of-tv-data-1445333401; *see also* Jason Aycock, *Comcast Ready to Monetize Volumes of Set-Top Viewing Data*, Seeking Alpha (Oct. 20, 2015), http://seekingalpha.com/news/2840916-comcast-ready-monetize-volumes-set-top-viewing-data.

> ment, and it's opened up opportunities we haven't had before."[197]

According to Cablevision's Tatta, having granular information about individual users comes in handy in marketing Cablevision services — why try to sell triple-play bundles to customers who already have triple-play bundles, after all. But media companies have aggressively sought this data, too.[198]

The article then quoted an industry analyst to explain the extraordinary granularity of the data collected from individual consumers:

> "In terms of the data cable operators get, it's not an estimate based on a sampling, the way Nielsen's is, but rather a full accounting of every set top box owner's behavior — what they watched, how long they watched, and whether they changed channels on the commercial break," said Alan Wolk, a senior analyst for The Diffusion Group.[199]

Cablevision's privacy policy[200] provides only the most general notice about the potential use of personally identifying information. Nothing in the generalized language suggests that video viewing habits — or other behavioral information — is collected in such granularity. Additionally, Cablevision's privacy policy states that it does not consider unique device identifiers, such as MAC addresses, personal private information — despite their valuable use in building profiles and identifying individuals.

We do not argue that Cablevision is violating existing law. To the contrary, our concern is that Cablevision's granular collection of personal information and unrestricted use does *not* violate existing, outdated FCC interpretations of section 631 and the current failure to apply § 222.

The Verizon supercookie experience described above,[201] coupled with Verizon's announcement that it will share all information it collects with its AOL online advertising subsidiary,[202] illustrates the need to invoke the

---

[197]Daniel Frankel, *From DAI to programmatic: Why advanced advertising is giving pay-TV operators a reason to stay in the video biz*, FIERCECABLE (Dec. 1, 2015), http://www.fiercecable.com/special-reports/dai-programmatic-why-advanced-advertising-giving-pay-tv-operators-reason-st.

[198]*Id.*

[199]*Id.*

[200]*Cablevision Customer Privacy Notice* (Mar. 20, 2015), https://www.optimum.net/pages/PrivacyExisting.html.

[201]*See supra* p. 51.

[202]Mlot, *supra* note 164.

FCC's authority to set rules for wireless services under § 303(b), to ensure that wireless companies offering bundled services with multiple affiliates do not likewise seek to exploit potential loopholes to harvest and exploit customer data Congress intended § 222 to protect.

7. The Commission Should Protect Competition By Supplementing Sections 222(a) and 222(b) With Rules Derived From Section 628 and Section 303(b)

As discussed at length in Part I above, while Congress intended to provide the maximum protection to consumers for their personal data, Congress *also* intended the FCC to use § 222(b) to protect competition. It is clear that where competing providers such as T-Mobile or Sprint must expose their proprietary broadband data to carriers such as AT&T and Verizon, that § 222(a)–(b) protects them as well. This must be equally true for exposure of information — including interconnection information — to competing broadband carriers under § 222(a). This becomes even more urgent as cable operators prepare to offer competing mobile services.[203]

A few illustrations will suffice to show the vulnerability of competing carriers. First, when a wireless carrier such as Sprint enters into a roaming agreement with another carrier, such as Verizon, Sprint must provide Verizon with traditional CPNI information, as well as information needed to provide the Sprint customer access to broadband services, so that the Sprint customer can use spectrum capacity on Verizon's network. While the Sprint customer roams on the Verizon network, Verizon is capable of collecting all the information about the customers use of broadband — for examples what applications the customer runs in the background, how often the Sprint customer checks email or social media — for the entire time the Sprint customer is connected to the carrier's network. Indeed, because data roaming may take place in the background, the customer herself may be entirely unaware that she is roaming.

Another example from the world of traditional CPNI the FCC must update for the broadband age is interconnection. All mobile broadband providers must connect the wireless tower that receives the mobile signal to a wireline connection to provide "backhaul" to the Internet. If T-Mobile

[203] *See* Mark Sullivan, *The planets are aligning for cable company mobile service*, VentureBeat (Mar. 5, 2015), http://venturebeat.com/2015/03/05/the-planets-are-aligning-for-cable-company-mobile-service/ ("The cable operators are in a great position to build a network that uses mainly Wi-Fi for data and voice, and then builds a thin LTE network on top to cover people who need mobile Internet outside the reach of those hotspots.").

purchases backhaul from its towers from a Title II carrier, an arrangement called "special access" or from a regulated Title II high-capacity Ethernet loop, the carrier purchasing backhaul must expose its data traffic to the carrier providing backhaul. By examining the nature of the traffic, including its point of origination and point of destination, the carrier providing the backhaul can collect information that will allow it to poach the competing carrier's customers. It can gauge the popularity of a rival's competitive offering and use that information to craft its own strategy. This is precisely the harm to competition that CPNI has always sought to prevent.

But protection of CPNI also applies to protection of mobile providers from a customer's residential broadband subscriber. To use Wi-Fi, a customer must expose the identifying information about the mobile device, which will allow the carrier to look up information about the mobile device and use that information to determine the rival mobile carrier.[204] The wireline provider can then offer competing mobile services, or make that information available to competing mobile service providers. In addition, the wireline operator can, through the Wi-Fi or Bluetooth connection with the devices, discover information with regard to applications using the Wi-Fi connection in preference to the licensed connection.

Many competing services, however, are arguably not covered by § 222(b). For example, alarm services are not providers of telecommunications services protected by § 222(b). Nor are providers of "smart" home monitoring services or other "Internet of Things" (IoT) applications. While this information is protected as the information of the broadband subscriber under § 222(a) and § 222(c), this may not adequately protect the proprietary information of competing services.

No service is more vulnerable to this harvesting of proprietary information than competing OTT video services. Nearly every residential broadband provider, and an increasing number of mobile broadband providers, offer their own streaming video services in direct competition with online streaming services such as Netflix, Amazon Prime, TwitchTV and Hulu. As described at length in Part III, broadband providers are uniquely capable, as a consequence of their unique relationship with the subscriber, to collect vast amounts of customer researcher by simply harvesting the information from their subscribers as they enjoy the compet-

[204]For example, if the wireline provider obtains the cell phone number associated with the device, the wireline provider can consult the local number portability database to determine the carrier to whom the number is assigned.

ing service. Worse, whatever information Netflix may obtain about a Netflix subscriber's viewing habits, the broadband provider can compile an even more granular profile by combining the subscriber's viewing habits across multiple platforms.

To adequately protect competition, particularly OTT video competition, the FCC should not rely exclusively on § 222. The FCC should affirmatively invoke its authority under section 628 to prohibit unfair and anticompetitive practices by video providers in the provision of video services, as well as its general authority under § 201(b).

Given the difficulty in policing the sharing of information between affiliates, the FCC should affirmatively prohibit sharing of CPNI between the BIAS provider and its affiliates. As the FCC recognized in the 1980s, sharing information derived from its carrier function with affiliates provides the carrier with an enormous anticompetitive advantage.

Conclusion

Congress placed with the FCC — and the FCC alone — the responsibility to ensure that the privacy of communications networks remains absolute. The FCC is uniquely designed to carry out this role, protecting our most uniquely sensitive information. All the information we protect today through specialized agencies — medical information, financial information, government information — effectively becomes accessible for any purpose if the means by which we send that information from one person to another can be compromised by the carrier.

The FTC plays an important and complementary role to the FCC in protecting consumer privacy, as it does with other specialized agencies such as the Consumer Financial Protection Board and the Food and Drug Administration. But the FTC has neither statutory authority nor agency capacity to police adequately the harvesting of personal information by broadband access providers. Nor does it have the statutory authority to protect services that compete with carriers who must expose their proprietary customer information to their rivals in order to provide service.

The objections of carriers that FCC action is neither necessary nor appropriate is plainly refuted by the existing collection practices of BIAS providers, even without consider the potential harm to privacy and competition they could do by using technologies such as deep packet inspection. The FCC must act swiftly, before the expectation of genuinely private communications becomes possible only for those able to afford it.

Privacy of communications is not a privilege to be granted as a matter of grace by benevolent carriers out of abiding concern for their customer's well being. It is not a luxury for which consumers should be expected to pay all the market can bear. It is, by statute, a right of all Americans. No corporate claims for "a level playing field" can overcome that statutory right. Nor can the persistence of threats to consumer privacy relieve the FCC of its statutory obligation to protect the statutory right of consumers to control their information under Section 222.

Bibliography

Cases

Amendment of Section 64.702 of the Commission's Rules & Regulations ("*Second Computer Inquiry*"),
79 F.C.C.2d 953 (1980) (Memorandum Opinion and Order) 10

Cellco Partnership v. FCC,
700 F.3d 534 (D.C. Cir. 2012) 21

Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.,
467 U.S. 837 (1984) 17

Citizens United v. Federal Election Commission,
558 U.S. 310 (2010) 43

City of Arlington v. FCC,
133 S. Ct. 1863 (2013) 17

FTC v. Verity International, Ltd.,
443 F.3d 48 (2d Cir. 2006) 30

FTC v. Wyndham Worldwide Corp.,
799 F.3d 236 (3d Cir. 2015) 21, 30, 33

In re Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable & Timely Fashion,
GN Docket No. 15-191 (Jan. 29, 2016) (2016 Broadband Progress Report) 22, 53

In re DoubleClick Inc. Privacy Litigation,
154 F. Supp. 2d 497 (S.D.N.Y. 2001) 46

In re Lifeline & Link Up Reform & Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund,
30 F.C.C. Rcd. 7818 (June 18, 2015) 17, 20, 60

In re Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers without Customers Consent Violates Section 222 of the Communications Act,
WC Docket No. 13-306 (FCC filed Dec. 11, 2013) 50

In re Petitions Seeking Amendment of Part 68 of the Commission's Rules Concerning Connection of Telephone Equipment, Systems & Protective Apparatus to Certain Private Line Services,
76 F.C.C.2d 246 (1980) 9

In re Protecting & Promoting the Open Internet,
30 F.C.C.R. 4681 (May 8, 2015) 51

In re Protecting & Promoting the Open Internet,
30 F.C.C. Rcd. 5601 (Feb. 26, 2015) 1, 19–20

In re Regulatory & Policy Problems Presented by the Interdependence of Computer & Communication Services & Facilities,
7 FCC 2d 11 (1966) (Notice of Inquiry) 9

In re Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information,
22 F.C.C. Rcd. 6927 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking), *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009) . . . . *passim*

In re Use of the Carterfone Device in Message Toll Services,
13 F.C.C.2d 420 (1968) 9

Kyllo v. United States,
533 U.S. 27 (2001) 48

National Cable & Telecommunications Ass'n v. FCC,
555 F.3d 996 (D.C. Cir. 2009) . . . . . *passim*

National Petroleum Refiners Ass'n v. FTC,
482 F.2d 672 (D.C. Cir. 1973) 29

Statutes

47 U.S.C. §§ 214, 301 38

47 U.S.C. §§ 214(a), 310(d) 39

—— § 222 . . . . . *passim*

—— § 222(a) . . . . . *passim*

—— § 222(a)–(b) 31, 67

—— § 222(b) 5–6, 16–17, 59, 67–68

—— §§ 222(b)–c 13

—— § 222(c) . . . . . *passim*

—— § 222(e) 16

—— § 225 18

—— § 225(b) 18

—— § 225(c)–(d) 18–19

—— § 227 40

—— § 251(a) 19

—— § 251(b)–(c) 19

—— § 252 12

—— § 252(f) 12

—— § 253 11

—— § 303(b) 6, 20, 67

—— § 303(r) 20

—— § 307(a) 21

Act of Sept. 29, 2003, Pub. L. No. 108-82, 117 Stat. 1006 40

Cable Communications Policy Act of 1984 § 631, 47 U.S.C. § 551 . 14, 21, 62, 65–66

Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 . 11

Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994, Pub. L. No. 103-297, 108 Stat. 1545 40

Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 40

Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (2007) 34

Wheeler-Lea Act of 1938, ch. 49, 52 Stat. 111 . . . . . 28, 30

Other Sources

Nader Ammari et al., The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy (2015), https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf 51

Shalini Ramachandran and Suzanne Vranica, *Comcast Seeks to Harness Trove of TV Data*, Wall St. J. (Oct. 20, 2015), http://www.wsj.com/articles/comcast-seeks-to-harness-trove-of-tv-data-1445333401 65

Jason Aycock, *Comcast Ready to Monetize Volumes of Set-Top Viewing Data*, Seeking Alpha (Oct. 20, 2015), http://seekingalpha.com/news/2840916-comcast-ready-monetize-volumes-set-top-viewing-data 65

Richard Bennett, *Bringing Privacy into the Open*, High Tech F. (Jan. 26, 2016),//hightechforum.org/bringing-privacy-into-the-open/ . . . 63

Mark Bergen & Alex Kantrowitz, *Verizon Looks to Target Its Mobile Subscribers with Ads* (May 21, 2014), http://adage.com/article/digital/verizon-target-mobile-subscribers-ads/293356/ 36

Ed Bott, *Why Does Comcast Need My Social Security Number?*, Ed Bott (June 29, 2005), http://www.edbott.com/weblog/2005/06/why-does-comcast-need-my-social-security-number/ 55

Julie Brill, Comm'r, Fed. Trade Comm'n, Address at the Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality: Net Neutrality and Privacy: Challenges and Opportunities (Nov. 19, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/881663/151119netneutrality.pdf 25

Cablevision Customer Privacy Notice (Mar. 20, 2015), https://www.optimum.net/pages/PrivacyExisting.html 66

Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014) 22

Customer Proprietary Network Information, 72 Fed. Reg. 31948 (FCC June 8, 2007) 34

Gerri Detweiler, *Will Bad Credit Stop You From Getting Cable?*, Credit.com (Mar. 24, 2014), http://blog.credit.com/2014/03/will-bad-credit-stop-you-from-getting-cable-78764/ 55

Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times Mag. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html 50

Elizabeth Dwoskin & Thomas Gryta, *AT&T Tacks a Privacy Charge on High Speed*, Wall St. J. (Feb. 18, 2015), http://www.wsj.com/articles/at-t-tacks-a-privacy-charge-on-high-speed-1424314904 . . . 52

Fact Sheet, *Chairman Wheeler Proposes New Rules for Protecting the Open Internet* (Feb. 4, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-331869A1.pdf 37

Nick Feamster, *Who Will Secure the Internet of Things?*, Freedom to Tinker (Jan. 19, 2016), https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/ 50

Fed. Trade Comm'n, Broadband Connectivity Competition Policy (2007), https://www.ftc.gov/reports/broadband-connectivity-competition-policy-staff-report 32

Fed. Trade Comm'n, How to Comply with the Privacy of Consumer Information Rule of the Gramm-Leach-Bliley Act (2002), https://www.ftc.gov/system/files/documents/plain-language / bus67 - how - comply - privacy - consumer - financial - information-rule-gramm-leach-bliley-act.pdf 25

Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (2010), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer - protection - preliminary - ftc - staff - report - protecting - consumer/101201privacyreport.pdf 29

Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (2012), *available at* https://www.ftc.gov / sites / default / files / documents / reports / federal - trade - commission - report - protecting - consumer - privacy - era - rapid - change-recommendations/120326privacyreport.pdf . . . 29–30, 32, 49, 59

Kevin Fitchard, *The Real Reason Verizon Bought AOL*, Fortune (June 24, 2015), http://fortune.com/2015/06/24/verizon-gains-aol/ 51–52

Lorenzo Franceschi-Bicchierai, *Nest Thermostat Leaked Zip Codes Over the Internet*, Vice: Motherboard (Jan. 20, 2016), http://motherboard.vice.com/read/nest-thermostat-leaked-home-locations-over-the-internet 50

Daniel Frankel, *From DAI to programmatic: Why advanced advertising is giving pay-TV operators a reason to stay in the video biz*, FierceCable (Dec. 1, 2015), http://www.fiercecable.com/special-reports/dai-programmatic-why-advanced-advertising-giving-pay-tv-operators-reason-st 66

GSM Ass'n, The Mobile Economy 2015 (2015), http://www.gsmamobileeconomy.com / GSMA _ Global _ Mobile _ Economy _ Report_2015.pdf 51

Stacey Higginbotham, *ISPs Really, Really Want to Be Able to Share Your Data*, Fortune (Apr. 28, 2015), http://fortune.com/2015/04/28/isps-share-your-data/ 52, 64

Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, Electronic Frontier Found. (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh 36

How Do I Configure My Router for Spotify?, Spotify Support (last visited Feb. 12, 2016), https://support.spotify.com/us/problems/#!/article/how-do-i-configure-my-router-for-spotify 47

H.R. 1555, 104th Cong. (1995) 13

H.R. Rep. No. 104-204 (1995) 13–16

Info. Scis. Inst., RFC 791, Internet Protocol (1981) 46

Info. Scis. Inst., RFC 793, Transmission Control Protocol (1981) 46

Joint Petition for Stay of United States Telecom Association et al., *In re* Protecting & Promoting the Open Internet, 30 F.C.C.R. 4681 (May 1, 2015) (No. 14-28) 51

Ryan Kearney, *Comcast Caught Hijacking Web Traffic*, Ryan Kearney (Jan. 9, 2013), http://blog.ryankearney.com/2013/01/comcast-caught-intercepting-and-altering-your-web-traffic/ 52

David Kravets, *Comcast Wi-Fi Serving Self-Promotional Ads via JavaScript Injection*, Ars Technica (Sept. 8, 2014), http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/ 52

Brian Krebs, *Privacy 101: Skype Leaks Your Location*, Krebs on Security (Mar. 13, 2013), http://krebsonsecurity.com/2013/03/privacy-101-skype-leaks-your-location/ 47

Letter from Am. Cable Ass'n et al., to Tom Wheeler, Chairman, Federal Communications Commission (Feb. 11, 2016), *available at* https://www.ncta.com/sites/prod/files/Privacy_Letter_021116.pdf . . . 3

Natasha Lomas, *Europe And US Seal 'Privacy Shield' Data Transfer Deal To Replace Safe Harbor* (Feb. 2, 2016), http://techcrunch.com/2016/02/02/europe-and-us-seal-privacy-shield-data-transfer-deal-to-replace-safe-harbor/ 20

Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 Geo. Wash. L. Rev. 1979 (2015) 29

Mary Madden, Pew Research Ctr., *Privacy and Cybersecurity: Key findings from Pew Research* (Jan. 16, 2015), http://www.pewresearch.org/key-data-points/privacy/ 23

Thomas Margoni & Mark Perry, *Deep Pockets, Packets, and Harbors*, 74 Ohio St. L.J. 1195 (2013) 49

Chris Matyszczyk, *Samsung's Warning: Our Smart TVs Record Your Living Room Chatter*, CNET (Feb. 8, 2015), http://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/ 28

Jonathan Mayer, *How Verizon's Advertising Header Works*, Web Pol'y (Oct. 24, 2014), http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/ 36

Robert McMillan, *Verizon's 'Perma-Cookie' Is a Privacy-Killing Machine*, Wired (Oct. 27, 2014), http://www.wired.com/2014/10/verizons-perma-cookie/ 36

Memorandum of Understanding from Fed. Commc'ns Comm'n & Fed. Trade Comm'n (Nov. 16, 2015), http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf 26, 41

Memorandum of Understanding from Fed. Trade Comm'n & Consumer Fin. Prot. Bureau (Mar. 6, 2015), *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/150312ftc-cfpb-mou.pdf 26

Stephanie Mlot, *Verizon to Share 'Super Cookie' Data with AOL's Ad Network*, PCMag (Oct. 7, 2015), http://www.pcmag.com/article2/0,2817,2492705,00.asp 51, 66

Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, Address at the 33rd Annual Institute on Telecommunications Policy & Regulation: FTC-FCC: When Is Two a Crowd? (Dec. 4, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/893473/151204plispeech1.pdf 31

Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010), http://www.uclalawreview.org/pdf/57-6-3.pdf 49

Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417 . . . . . 50, 53

Open Tech. Inst., New Am. Found., The FCC's Role in Protecting Online Privacy (2016), https://www.newamerica.org/oti/the-fccs-role-in-protecting-online-privacy/ 57–58

Lara O'Reilly, *Fresh from being bought by Verizon, AOL is reportedly preparing to acquire mobile ad tech company Millennial Media for $300 million*, Bus. Insider (July 9, 2015), http://www.businessinsider.com/report-aol-to-buy-millennial-media-for-300-million-2015-7 51

Ashley Parker, *"Corporations Are People," Romney Tells Iowa Hecklers Angry Over His Tax Policy*, N.Y. Times, Aug. 12, 2011, at A16 . . 43

Rob Pegoraro, *How to Turn Off Verizon's 'Supercookie' Tracking*, USA Today (Apr. 5, 2015), http://www.usatoday.com/story/tech/personal/2015/04/05/verizon-supercookie/25247591 37

Petition for Declaratory Ruling, *In re* Petition of Pub. Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecomms. Providers without Customers Consent Violates Section 222 of the Commc'ns Act, WC Docket No. 13-306 (FCC Dec. 11, 2013) 50

Petition for Partial Reconsideration of CTIA — The Wireless Association, *In re* Lifeline & Link Up Reform & Modernization, Telecomms. Carriers Eligible for Universal Serv. Support, Connect Am. Fund, 30 F.C.C. Rcd. 7818 (Aug. 13, 2015) (WC Docket Nos. 11-42, 09-197, 10-90) 17, 20, 60

Jonathan B. Postel, RFC 821, Simple Mail Transfer Protocol (1982), https://www.ietf.org/rfc/rfc821.txt 47

Press Release, *Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy* (May 20, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0520/DA-15-603A1.pdf 2

Press Release, European Comm'n, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield* (Feb. 2, 2016), *available at* http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en 20

Edith Ramirez, Chairwoman, Fed. Trade Comm'n, *The FTC: A Framework for Promoting Competition and Protecting Consumers*, 83 Geo. Wash. L. Rev. 2049 (2015) 29

J. Reynolds & J. Postel, RFC 1700, Assigned Numbers (1994), https://www.ietf.org/rfc/rfc1700.txt 47

James Robinson, *The 21st Century Privacy Coalition Doesn't Really Care About Your Privacy*, Pando (June 4, 2014),/2014/06/03/despite-team-up-for-the-21st-century-privacy-coalition-americas-telecoms-giants-really-arent-looking-out-for-your-privacy/ 26

S. 652, 104th Cong. (1995) 12–13

Sandvine Intelligent Broadband Networks, Global Internet Phenomena Spotlight: Encrypted Internet Traffic (2015), https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf 48

Natasha Singer & Brian X. Chen, *Use of Mobile "Supercookies" Is Seen as a Threat to Privacy*, N.Y. Times, Jan. 25, 2015, at B2 54

Ms. Smith, *Security and Privacy Checklist for Smart Home, IoT Devices*, Network World (Dec. 9, 2015), http://www.networkworld.com/article/3013512/security/security-and-privacy-checklist-for-smart-devices-50-million-to-be-sold-over-holidays.html 28

Mike Snider, *Verizon to Let Users Opt Out of "Super Cookie" Identifier*, USA TODAY, http://www.usatoday.com/story/tech/personal/2015/02/01/verizon-opt-out-supercookies/22697549/ 37

Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014) 30

Dawn Xiaodong Song et al., *Timing Analysis of Keystrokes and Timing Attacks on SSH*, 10 Proc. Conf. on USENIX Security Symp. No. 25 (2001), *available at* https://www.usenix.org/legacy/events/sec01/full_papers/song/song.pdf 48

Elizabeth Weise, *AT&T Ends Tracking of Customers by "Supercookie"*, USA Today, http://www.usatoday.com/story/tech/2014/11/14/att-supercookies-tracking/19041911/ 38

Tom Wheeler, *FCC Chairman Tom Wheeler: This Is How We Will Ensure Net Neutrality*, Wired (Feb. 4, 2015), http://www.wired.com/2015/02/fcc-chairman-wheeler-net-neutrality/ 37

Tom Wheeler, Net Effects: The Past, Present, and Future Impact of Our Networks (2013), *available at* https://transition.fcc.gov/net-effects-2013/NET_EFFECTS_The-Past-Present-and-Future-Impact-of-Our-Networks.pdf 38

Chris Wilson, *What's "Port 25," and What Does It Have to Do with E-mail Spam?*, Slate Mag. (July 1, 2008), http://www.slate.com/articles/news_and_politics/explainer/2008/07/the_spam_superhighway.html 47

Tim Wu, The Master Switch (2010) 9

T. Ylonen & C. Lonvick, RFC 4253, The Secure Shell (SSH) Transport Layer Protocol (2006), https://www.ietf.org/rfc/rfc4253.txt 48

Colophon

This white paper is set in Linux Libertine, with titles set in Adobe Source Sans Pro. The text was set using LaTeX.