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

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.