Reply Comments of

TechFreedom

Berin Szóka[1] & Tom Struble[2]

Competitive Enterprise Institute

Ryan Radia[3]

In the Matter of

Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

WC Docket No. 16-106

July 6, 2016

---

[1] Berin Szóka is President of TechFreedom, a nonprofit, nonpartisan technology policy think tank. He can be reached at bszoka@techfreedom.org.

[2] Tom Struble is Policy Counsel at TechFreedom. He can be reached at tstruble@techfreedom.org.

[3] Ryan Radia is Research Fellow and Regulatory Counsel at the Competitive Enterprise Institute. He can be reached at ryan.radia@cei.org.

Table of Contents

I. Introduction 2

II. The FCC Should Not Have Rushed to Begin this Proceeding, and Should Not Rush to Finish It 4

A. The FCC Did Not Need Regulations to Protect Consumers, but Could Have Enforced Title II Statutory Provisions Case by Case 4

B. The FCC Should Have Resolved Ripe Questions About Its Legal Authority Before Issuing This NPRM 7

C. The Commission Should Have Waited for Resolution of Two Legal Challenges to Its Legal Authority 8

D. The FCC Can Resolve these Process Failures With a Further Notice of Proposed Rulemaking 10

III. How the FCC Might Proceed Case by Case 11

A. What The Commission Believes It Can Do 11

B. Fair Notice and Limits Upon the FCC's Ability to Impose Penalties Absent Rulemaking 12

C. What this Means for the FTC 15

IV. The FCC Should Harmonize Its Approach with the FTC 15

A. The FCC Should Follow the FTC's Deception Policy Statement 15

B. Why Should the FCC Follow the FTC's Approach? 17

C. The FCC Should Follow the FTC's Unfairness Policy Statement 19

D. The FCC Should Adopt the Substantive Test of Section 5 If It Issues Rules 21

E. The FCC Incorrectly Cites the FTC's Big Data Report on Discounts 24

V. Section 705 of the Communications Act Actually *Curtails* the FCC's Authority. 24

A. After Enacting Section 705 in 1934, Congress Narrowed It in 1968 25

B. The Wiretap Act Allows Broadband Providers to Intercept the Communications of Subscribers Who Have Given Their Consent 27

C. The Proposed Rules Conflict with the Wiretap Act Insofar as They Regulate Broadband Providers' Interception of Content 29

VI. Section 706 of the Telecom Act Is Not an Independent Grant of Regulatory Authority. 32

VII. Legal Uncertainty over Whether 201(b) Covers Marketing Suggests the FCC Should Harmonize with the FTC. 37

VIII. Conclusion 38

I. Introduction

Chutzpah, wrote Leo Rostein in his 1968 classic, *The Joys of Yiddish*, is "that quality enshrined in a man who, having killed his mother and father, throws himself on the mercy of the court because he is an orphan."[4]

On privacy, the FCC has reached new heights in chutzpah: having robbed the FTC of its "jurisdictional lunch money" over broadband,[5] the FCC claimed it needed to issue broadband privacy regulations to fill a vacuum in consumer protection — and that it would simply recreate the FTC's approach. The Chairman told the Senate Judiciary Committee the FCC's approach "is firmly rooted in the privacy protection work done by the FTC in the exercise of the FTC's general consumer protection jurisdiction."[6]

But the FCC is doing far more than simply replicating the FTC's approach in an area that the FTC can no longer regulate (because of the FCC). The FCC is not merely replacing case-by-case enforcement of general standards with a more specific rulemaking, it is inventing new requirements based on new substantive standards that would give the FCC even more discretion than the sweeping discretion previously enjoyed by the FTC.

Most of all, it is clear that the FCC plans, in the inevitable legal challenge, to justify this bait-and-switch by throwing itself on the mercy of the court — with its usual claims of deference in interpreting (allegedly) ambiguous statutory provisions.

We believe the FCC should go back to the drawing board, revise its plans to bring its approach more in line with the FTC, and issue a Further NPRM, because full harmonization:

1. Would produce better outcomes for consumers;
2. Is what the Chairman had promised;
3. Would restore the *status quo ante* reclassification;
4. Would be competitively neutral, treating broadband companies differently from edge companies only when truly warranted; and
5. Would ensure that there would be no substantive change in privacy oversight if the FCC ultimately loses on reclassification at the full D.C. Circuit or Supreme Court.

---

[4] LEO ROSTEIN, THE JOYS OF YIDDISH (1968).

[5] Joshua Wright, *Twitter* (Jan. 21, 2015, 9:37 PM), *available at* https://goo.gl/6JSfwF.

[6] Testimony of Tom Wheeler, Chairman, Fed. Comms. Comm'n, *Examining the FCC's Proposed Privacy Rules: Hearing Before the Committee on the Judiciary, Subcommittee on Privacy, Technology & the Law, United States Senate*, at 3 (May 11, 2016), *available at* https://goo.gl/5k0KhN.

As the Intervenor in the legal challenge to the Open Internet Order (on behalf of Silicon Valley entrepreneurs and investors, and Cari.net, a data center and hosting provider),[7] TechFreedom plans to take the case to the full D.C. Circuit for rehearing — and on to the Supreme Court, if necessary. The majority simply did not address our core arguments,[8] that the FCC should not apply the familiar two-step test of *Chevron*, because the court should, at what has been called "step zero" of *Chevron*, decline to apply that test.[9] Even if reclassification does make it to "step two," Judge Williams amply explained why the FCC's interpretation of the statute was the epitome of arbitrary and capricious reasoning.[10]

If the FCC ultimately loses on reclassification, this entire proceeding will be unnecessary — because the FCC will lose authority over broadband providers as "common carriers" and the FTC will automatically regain the authority it had long exercised. Indeed, in our view, the Commission would have no authority to regulate broadband privacy whatsoever because the other statutory provisions cited by the FCC do not provide the Commission the authority it would need for this proposal.

In any event, the FCC should have waited for that litigation to be resolved at the full D.C. Circuit and Supreme Court before issuing this proposal. Having pleaded with the Commission for an extension of this deadline[11] and been rebuffed, we declined to spend our limited institutional resources analyzing the complex issues raised by the FCC's interpretation of these provisions in the initial comment round — which closed shortly before the decision was issue.

Here, we note that, if the Commission can use the provisions of Title II it cites (as well as other provisions) to regulate broadband privacy and data security, the Commission itself believes it can do so without issuing formal rules, through case-by-case enforcement that includes monetary penalties — and, indeed, has already done so. Thus, there was no vacuum in consumer protection requiring the Commission to rush to issue this proposal.

---

[7] *See Motion of TechFreedom, et al. for Leave to Intervene in* U.S. Telecom Ass'n v. FCC, Case No. 15-1063 (D.C. Cir., June 8, 2015), *available at* http://goo.gl/z5MyTf.

[8] U.S. Telecom Ass'n v. FCC, No. 15-1063, slip op. at 55 (D.C. Cir. June 14, 2016), *available at* https://goo.gl/Wt3T7q.

[9] *Brief for Intervenors for Petitioners TechFreedom, et al.*, U.S. Telecom Ass'n v. FCC, Case No. 15-1063 (D.C. Cir., Aug. 6, 2015), http://goo.gl/2nBHDE; *Reply Brief for Intervenors for Petitioners TechFreedom, et al.*, U.S. Telecom Ass'n v. FCC, Case No. 15-1063 (D.C. Cir., Oct. 5, 2015), *available at* https://goo.gl/8Oi8M1.

[10] U.S. Telecom Ass'n v. FCC, No. 15-1063, slip op. (D.C. Cir. June 14, 2016) (Williams, J. dissenting).

[11] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Written Ex Parte of TechFreedom*, WC Docket No. 16-106 (Apr. 19, 2016) ["TechFreedom Ex Parte"], *available at* http://goo.gl/M894Ss (supporting ANA's requested extension in the instant proceeding).

We urge the Commission to truly harmonize its approach with that of the FTC as follows:

1. Use the authority the FCC claims under Title II to guide case-by-case enforcement of ISPs' privacy and data-security practices.
2. To the extent reclassification fails, desist from further action on this proceeding;
3. To the extent the full D.C. Circuit and Supreme Court uphold reclassification (or simply let the panel decision stand), issue a Further Notice of Proposed Rulemaking that:
    a. Makes clear the FCC will, in general, follow the same substantive standards of the FTC's Unfairness and Deception Policy Statements, and Section 5(b) and (n) of the FTC Act;
    b. Clearly grounds its analysis of proposed rules in these standards; and

II. The FCC Should Not Have Rushed to Begin this Proceeding, and Should Not Rush to Finish It

Issuance of this NPRM[12] was premature. It was probably also unnecessary, at least if it serves as something other than what the Commission really should have done: issuing a Notice of Inquiry.

At a minimum, the FCC should first have ruled on a pending Petition for Reconsideration filed by CTIA last October.[13] The first two matters will decide what legal authority the FCC has here, if any; the first of them, whether there is any gap in consumer protection that the FCC needs to fill; and the third, how the FCC may exercise whatever legal authority it might have over privacy.

A. The FCC Did Not Need Regulations to Protect Consumers, but Could Have Enforced Title II Statutory Provisions Case by Case

We are mystified by the FCC's insistence on rushing out this NPRM. There is simply no need for the FCC to rush to issue final rules, or forego issuing a Further NPRM (as will be necessarily to develop a proper record), because the FCC can already protect consumers through case-by-case adjudication — and could continue to do so while the question of Title II broadband reclassification works its way through the D.C. Circuit and Supreme Court.

---

[12] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, 31 FCC Rcd 2500 (2016) ["NPRM"], *available at* https://goo.gl/UXjF05.

[13] Lifeline and Link Up Reform and Modernization, *CTIA Petition for Partial Reconsideration*, WC Docket No. 11-42 (Aug. 13, 2015) ["CTIA Petition for Reconsideration"], *available at* http://goo.gl/sgU9bN.

It was only the Open Internet Order's reclassification of broadband that made it necessary for the FCC to do *something* about broadband privacy and data security, but nothing about the Order requires a *rulemaking*. The Order offered broad forbearance, including from applying the FCC's current rules based on Section 222,[14] but did *not* forbear from Sections 222 or 201 themselves. Between these two sections, the Commission can adequately police privacy and data security practices on a case-by-case basis, even in the absence of FCC data-security or privacy regulations. The Commission has already taken this approach, grounded directly in Title II rather than rules issued pursuant to it, in three recent decisions:

- *TerraCom* (October 2014): adequacy of data security for Lifeline voice service, based on Sections 222(a) and 201(b);[15]
- *Cox* (November 2015): adequacy of data security against pretexting attack on Cox's cable billing system, premised on Sections 631(c)(1), 222(a), and 201(b);[16]
- *Verizon* (March 2016): insertion of "supercookies" into mobile wireless traffic to service targeted advertising, premised on the Open Internet Order's Transparency Rule, as well as Section 222(b).[17]

It is worth noting that only one of these was actually about broadband privacy, and involved conduct that was neither clearly illegal nor clearly harmful. In other words, not only has the Commission already claimed the statutory tools to protect consumers case by case, but what's more: there is no clear problem crying out for the FCC to rush through a rulemaking, let alone one so draconian as what the FCC has proposed.

What could the Commission *not* do without formal rules? As discussed below, the Commission believes it can impose monetary penalties even without formal privacy or data-security rules, and has already done so in the proceedings cited above — or, where it declined to impose fines for the first time it sanctioned conduct directly under Section 201(b) or 222(a), it put companies on notice that it *would* impose fines in similar situations in the future involving other companies.[18] Thus, the Commission carries a large cudgel with which to deter unfair or deceptive broadband data practices — a cudgel even the FTC does

---

[14] Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, GN Docket No. 14-28, ¶ 467 (July 17, 2014) ["OIO"], *available at* https://goo.gl/QafQCE.

[15] TerraCom NAL, *supra* note 21.

[16] In re Cox Communications, Inc., *Order*, EB-IHD-14-00017829 (Nov. 5, 2015), *available at* https://goo.gl/m0W0FI.

[17] In re Cellco Partnership, d/b/a Verizon Wireless, *Order*, EB-TCD-14-00017601 (Mar. 7, 2016) ["Verizon Order"], *available at* https://goo.gl/Eb09oS.

[18] *See supra* at 8.

not have (since the FTC lacks civil penalty authority for first time violations of Section 5). So why could the Commission not adequately protect consumers using that cudgel through case-by-case enforcement?[19]

At most, we see one clear difference: It is true that there would not be a formalized, uniform set of data-breach-notification requirements for broadband companies. Instead, the FCC could, as it did in TerraCom, develop substantive requirements as to what constitutes adequate notification piecemeal. But, as long as the FCC did not preempt state breach-notification requirements, those laws would still apply. At worst, there would be something of a patchwork of such laws, but this would be a burden borne primarily (if not entirely) by the companies themselves in the form of additional compliance costs. Using Section 201(b), the Commission could likely supplement these laws with its own enforcement of them, holding that the failure to comply with the applicable state data-breach-notification laws is itself an unjust and unreasonable practice.

Given the absence of any systemic problems involving broadband privacy or data security, this minor difference is not enough to justify the FCC's rush in proceeding with this rulemaking. The FCC waited over a year to issue this NPRM, while bringing a single broadband privacy complaint (*Verizon*) — and this for ambiguous conduct. What difference would another few months have made?

If the Commission really believes that "both consumers and Internet Service Providers (ISPs) would benefit from additional, concrete guidance explaining the privacy responsibilities created by the Communications Act,"[20] why could it not have responded to the CTIA Petition during this period? If the Commission is so sure of its legal authority under Sections 222(a) and 201(b), both here and in the three enforcement actions cited above, why could it not have addressed the questions raised by CTIA's Petition *before* issuing this NPRM?

---

[19] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Comments of the International Center for Law & Economics, at 2–3 (May 27, 2016), *available at* https://goo.gl/m0AzVK ("[A]ll of the foregoing is particularly perplexing in light of the fact that the Commission is perfectly capable of regulating privacy under § 201(b) on a case-by-case basis — as it did in *TerraCom*. Compared to blunt, prescriptive rules, such an approach reduces the likelihood that the Commission will inadvertently create more consumer harm than benefit. At the same time, the Commission has not shown that regulatory efficacy, administrative efficiency or anything else demands such rules. Particularly given *TerraCom* and the demonstrated ability of the Commission to handle harms as they arise *even absent prescriptive rules*, the need for these aggressive new rules simply cannot be justified.").

[20] NPRM ¶ 2.

B. The FCC Should Have Resolved Ripe Questions About Its Legal Authority Before Issuing This NPRM

Why did the Commission rush to propose these rules without first addressing a ripe Petition for Reconsideration before it about the legal authorities now cited by the Commission for its proposed rules? Doing so would have allowed commenters in this proceeding a far clearer understanding of the authority the Commission believes it has, the basis for that belief, and how it believes that authority could be used in the future.

In October 2014, the FCC invoked Sections 222(a) and 201(b) as the basis for an enforcement action against TerraCom for failing to provide "reasonable data security" regarding the information provided by Lifeline applicants for determining their eligibility for subsidized telephone service.[21] The *TerraCom* Notice of Apparent Liability quoted the FCC's 2007 CPNI Order, saying "Every telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI"[22] — a "duty owed to other carriers, equipment manufacturers, and customers."[23]

In June, 2015, the FCC again invoked these sections, declaring that "pursuant to section 222 of the Act, [carriers] have a duty to protect 'the confidentiality of proprietary information' of customers,"[24] and that "[Section 201(b)'s] requirement that such practices be 'just and reasonable,' also imposes a duty on [carriers] related to document retention security practices."[25]

CTIA filed a Petition for Partial Reconsideration, objecting to both claims of statutory authority.[26] The FCC has yet to respond. While the FCC is under no statutory obligation to re-

---

[21] In re TerraCom, Inc. & YourTel America, Inc., *Notice of Apparent Liability for Forfeiture*, File No. EB-TCD-13-00009175 (Oct. 24, 2014) ["TerraCom NAL"], *available at* https://goo.gl/jRBvYO.

[22] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, *Report and Order and Further Notice of Proposed Rulemaking*, CC Docket No. 96-115, ¶ 6 (rel. Apr. 2, 2007), *available at* https://goo.gl/mw8jiy.

[23] *Id* n.6. The Order claimed that "section 222(a) … provides ample authority for the Commission to require carriers to report CPNI breaches to law enforcement and prohibit them from disclosing breaches to their customers until after law enforcement has been notified," *Id*. ¶ 27, and that "section 222 … [requires] that carriers take reasonable measures to discover and protect against activity that is indicative of pretexting," *Id*. ¶ 33, and "section 222 … CPNI constitutes sensitive information that is protected under [Section 222(a).]" *Id.* ¶ 48.

[24] Lifeline and Link Up Reform and Modernization; Telecommunications Carriers Eligible for Universal Service Support; Connect America Fund, *Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order*, 30 FCC Rcd 7818, ¶ 234 and n.456 (2015) ["Order on Reconsideration"], *available at* https://goo.gl/fGtZOR.

[25] *Id*. ¶ 235 and n.458.

[26] CTIA Petition for Reconsideration, *supra* note 13.

spond to petitions for reconsideration,[27] the agency should have addressed the legal questions raised by the CTIA Petition prior to launching this proceeding — which hinges on those very questions.

C. The Commission Should Have Waited for Resolution of Two Legal Challenges to Its Legal Authority

The recent decision by a D.C. Circuit panel to uphold the FCC's 2015 Open Internet Order raised nearly as many questions as it answered.[28] Yes, the two judge majority deferred to the FCC's reclassification of broadband, and to the rules issued under that purported authority, but Judge Williams' scathing dissent calls that victory into question[29] — not just on the "net neutrality" (and additional) rules but on reclassification itself, the rationale for which Williams blasted as arbitrary and capricious.[30] As an Intervenor in the case, TechFreedom plans to file a petition for *en banc* review by the full D.C. Circuit, and the Petitioners may do the same. If the full appeals court agrees to rehear the case, a decision will likely take another year, at minimum. Either way, an appeal to the Supreme Court will follow, by one side or the other.

The FCC should have waited to see whether the D.C. Circuit would rehear the case or whether the Supreme Court would grant cert. If either happens, issuing this NPRM would have been premature — and, as explained above, unnecessary. At this point, the Commission should stay its hand from issuing final rules until we know whether the case will proceed. If the concern were that either round of litigation would take too long because, despite the above, the FCC feels it needs to write rules in order to protect consumers, the FCC should clearly explain why this is so — and it should also wait to proceed with issuing an order until. If the FCC is confident it will prevail, it has little to lose by waiting until mid-September (the window for cert petitions being 90 days).

If either court ultimately blocks reclassification of broadband, that would of course render moot this proceeding, while also barring the FCC from using Title II, except perhaps as a hook for ancillary authority. Even if a court blocked reclassification only of mobile, but not fixed, broadband, that would raise serious questions about the right approach for the FCC to take in this proceeding.

---

[27] The Commission's rules say the agency, or a Bureau, as appropriate, will respond to a properly filed petition for reconsideration, but set forth no timeline for doing so, 47 C.F.R. 1.429, and nothing in the Communications Act compels it to do so.

[28] U.S. Telecom Ass'n v. FCC, *supra* note 8, at 55.

[29] *Id.*, slip op. at 1 (Williams, J. dissenting).

[30] *Id.*, slip op. at 24 (Williams, J. dissenting).

Also, the Sixth Circuit is expected soon to release its decision on the FCC's 2015 preemption of state laws regarding government-owned broadband.[31] While it seems likely that the FCC will lose simply on federalism grounds, for lack of a "clear statement" to override state sovereignty (by re-allocating decision-making power regarding government-owned broadband from state legislatures to the municipalities created by the states), the court may also rule on the underlying question of whether Section 706 confers any independent grant of authority at all — as we believe it does not.[32] If so, this would remove one of the legal bases for the NPRM. While the D.C. Circuit[33] and Tenth Circuit[34] have upheld the FCC's interpretation of Section 706 as an independent grant of regulatory authority, we maintain that the discussions of Section 706 in both decisions are dicta, as they were unnecessary to the holdings of those cases, and therefore should not be considered binding precedent. And neither decision addressed the statutory and constitutional questions we have raised before the Sixth Circuit, as summarized below.[35]

In short, before rushing into this proceeding, the FCC should have responded to the CTIA Petition, waited until the full D.C. Circuit and Supreme Court had indicated whether they would hear the case, and until the Sixth Circuit had issued its decision. We supported a requested extension of the filing deadline on these grounds, while also noting that the FCC's comment system had accumulated a large backlog of comments (meaning, at a minimum, that reply commenters in this proceeding would likely have less time to review and respond to comments than allowed by the FCC's reply-comment window).[36] But the Commission summarily rejected the requested extension,[37] despite acknowledging the true scale of the backlog (74,000 comments) less than two weeks later.[38]

---

[31] City of Wilson, North Carolina Petition for Preemption of North Carolina General Statute Sections 160A-340 *et seq.*; The Electric Power Board of Chattanooga, Tennessee Petition for Preemption of a Portion of Tennessee Code Annotated Section 7-52-601, *Memorandum Opinion and Order*, WC Docket Nos. 14-115; 14-116 (rel. Mar. 12, 2015), *available at* https://goo.gl/YkdbHC.

[32] *See infra* at 8.

[33] *See* Verizon v. FCC, 740 F.3d 623, 636–42 (D.C. Cir. 2014).

[34] *See* In re FCC 11-161, 753 F.3d 1015, 1049–54 (10th Cir. 2014).

[35] *See infra* at 15.

[36] TechFreedom Ex Parte, *supra* note 11.

[37] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Order*, WC Docket No. 16-106 (Apr. 29, 2016), *available at* https://goo.gl/C0rSV2 (denying the requested extension).

[38] *See, e.g.*, John Eggerton, *FCC: Glitch, Backlog Delaying Broadband Privacy Comments*, BROADCASTING & CABLE (May 12, 2016), *available at* http://goo.gl/QLrwkN (quoting FCC Press Secretary Kim Hart acknowledging the significant backlog of yet-to-be-posted comments filed with the FCC in various proceedings).

D. The FCC Can Resolve these Process Failures With a Further Notice of Proposed Rulemaking

Is the Commission simply using the NPRM's questions about legal authority to help inform its decision on the CTIA Petition? It has already put that Petition out for public comment once. Now, it is true that this NPRM raises a broader set of legal issues, since that Petition concerned the use of Sections 201(b) and 222(a) as the bases for data-security and data-breach-notification regulations, while this NPRM concerns a broader set of privacy rules based on those purported statutory authorities, as well as other statutory authorities. But these broad and weighty legal questions are the sort of questions that should be addressed through a Notice of Inquiry (NOI) rather than an NPRM.

This is simply the latest example of the Commission using NPRMs when it should be using NOIs.[39] Whatever discretion the Commission enjoys under the Administrative Procedure Act[40] to configure its rulemaking process, this pattern denies regulated parties adequate opportunity to shape the FCC's proposal, insofar as the FCC merges analysis of basic legal questions with analysis of its proposed rules into a single round of comments. Once the NPRM is issued, the gun is loaded, and the Commission may fire at any time. Ready, fire, aim![41]

Fortunately, the FCC does not *have* to fire yet. It could take the time to aim before firing (i.e., issuing rules), simply by issuing a FNPRM that more clearly articulates the Commission's interpretations of Sections 222(a) and 201(b) based on comments filed in this comment cycle as well as the D.C. Circuit's ruling on the Open Internet Order. Although that decision came down before the reply-comment deadline in this proceeding, the Commission would benefit from seeking input in a *full* comment round with a FNPRM that incorporates the Commission's analysis of that decision.

This is not a dilatory tactic — an attempt to simply run out the clock until the FCC potentially changes hands under a new administration. There is still plenty of time for the Commission to complete this rulemaking well before any possible change in administration.

---

[39] *See, e.g.*, Protecting and Promoting the Open Internet, *Notice of Proposed Rulemaking*, GN Docket No. 14-28, at 92 (May 15, 2014), *available at* https://goo.gl/FIowH0 (Commissioner Rosenworcel, concurring) ("I would have done this differently. Before proceeding, I would have taken the time to understand the future[,]" and "taken time for more input.").

[40] Pub. L. No. 79-404, 60 Stat. 237 (1946) (codified as amended at 5 U.S.C. § 551 *et seq.*).

[41] *See also* TechFreedom, *FCC Violates Basic Legal Principles in Rush to Regulate Set-Top Boxes* (Feb. 18, 2016), *available at* http://goo.gl/0aQMQc ("This is simply the latest example of the FCC abusing the rulemaking process by bypassing the Notice of Inquiry… Every time the FCC does this, it means the gun is already loaded, and 'fact-finding' is a mere formality.").

III. How the FCC Might Proceed Case by Case

There is little question that the FCC can enforce Section 201(b) on a case-by-case basis, as the FTC does with Section 5. The FCC has long "found that unfair and deceptive practices by interstate common carriers constitute unjust and unreasonable practices under Section 201(b)…"[42] The FCC has also begun building a kind of unfairness doctrine premised on Section 222(a), all without — as of yet — issuing any formal rules.

A. What The Commission Believes It Can Do

In general, administrative agencies have discretion to regulate through either rulemaking or adjudication.[43] An agency's "judgment that adjudication best serves this purpose is entitled to great weight."[44] Under what circumstances the Commission can impose penalties in such enforcements is a more difficult question, hinging on whether, in the absence of regulations, the Commission has otherwise provided sufficient "fair notice" of what these sections require in order to meet constitutional standards of due process. As the Commission itself noted in the 2015 Open Internet Order (explaining why it did not believe Section 706 alone was an adequate basis for regulating privacy, and thus why the Commission declined to forbear from imposing Section 222 on broadband):

> [T]he Commission cannot impose a penalty in the absence of "fair notice of what is prohibited."[45]

The Commission clearly believes it can impose such monetary penalties for data-security cases brought under Section 222(a) and for data-security and privacy cases brought under Section 201(b) — if not the first time it sanctions particular conduct, then the second time it brings such an enforcement action (not necessarily against the same company). In *TerraCom*, for example, the FCC imposed $10,000,000 in total fines for the companies' allegedly unreasonable data security and for failing to notify customers of data breaches: $8,500,000 for violation of Section 222(a),[46] and an additional $1,500,000 for violation of Section 201(b).[47] The Commission was careful to distinguish between what amounted to its decep-

---

"[42] In re Advantage Telecommunications Corp., *Notice of Apparent Liability for Forfeiture*, File No. EB-TCD-12-00004803, at ¶ 10 and n.27 (rel. May 9, 2013), *available at* http://goo.gl/oCOELe (summarizing such cases).

[43] *See, e.g.*, Nat'l Labor Relations Bd. v. Bell Aerospace Co., 416 U.S. 267, 290–95 (1974).

[44] *Id*. at 294.

[45] OIO n.1394 (citing FCC v. Fox Television Stations, 132 S. Ct. 2307, 2317 (2012)).

[46] Terracom NAL, *supra* note 21, ¶ 52.

[47] *Id.* ¶ 53.

tion claim (not novel, thus appropriately the basis for a penalty) and its unfairness claim (novel):

> Accordingly, for the continuing violation of Section 201(b) caused by the Companies' false and misleading privacy policies, we propose a forfeiture of $1,500,000. However, in light of the fact that this is the first time we declare a carrier's practices unjust and unreasonable under Section 201(b) for failures related to (i) data security and (ii) notice to consumers in connection with a security breach, combined with the fact that we are imposing $10 million in penalties for the other violations at issue here, we exercise our discretion not to assess a forfeiture here for these apparent violations. *But carriers are now on notice that in the future we fully intend to assess forfeitures for such violations*.[48]

By contrast, in *Verizon*, the FCC appears to have grounded its $1,350,000 in the Open Internet Order's transparency rule.[49] And in *Cox*, the Commission merely applied its existing cable CPNI rules.[50]

Elsewhere, the Commission has explained its approach to this issue, such as in its 2015 Lifeline Order (on enforcing new recordkeeping requirements):

> This interpretation is a permissible, perspective [sic] application of a new rule because it does not affect or penalize past behavior but instead affects only conduct going forward. *Cf*. Connect America Fund et al., WC Docket No. 10-90, et al., *Third Order on Reconsideration*, 27 FCC Rcd 5622, 5628, ¶ 14 (2012) (Making a similar interpretation in the high-cost context).[51]

B. Fair Notice and Limits Upon the FCC's Ability to Impose Penalties Absent Rulemaking

These are difficult issues. We note and largely share Commissioner O'Rielly's concerns:

> I continue to be troubled when the Commission seeks to impose a fine in the absence of any rules. If section 201 is truly "ambiguous enough that

[48] *Id.* ¶ 53 (emphasis added).

[49] *Verizon Order*, *supra* note 17, at ¶¶ 2, 5.

[50] *Cox Order*, *supra* note 16, at ¶ 3.

[51] Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund, *Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order*, WC Docket Nos. 11-42, 09-197, 10-90, at n.463 (rel. June 22, 2015) ["Lifeline Order"], *available at* https://goo.gl/fGtZOR.

> unjust or unreasonable practices can encompass a broad range of activities" then how are providers supposed to know what conduct will run afoul of it?[52]

The FTC has not had to confront this question, because the agency cannot, by statute, impose civil penalties for first-time violations of Section 5—only for violation of consent orders. But the FTC *has* confronted the more general problem of whether its case-by-case enforcement of Section 5 meets fair-notice requirements. This past year the Third Circuit rejected Wyndham's fair-notice arguments, explaining that the degree of fair notice required is inversely correlated with the deference given the agency by the courts:

1. ***Skidmore***: "where an agency administers a statute without any special authority to create new rights or obligations … the courts give respect to the agency's view to the extent it is persuasive, but they retain the primary responsibility for construing the statute."[53] Accordingly, "a party lacks fair notice when the relevant standard is 'so vague as to be no rule or standard at all.'"[54]
2. ***Chevron***: "where an agency exercises its authority to fill gaps in a statutory scheme. There the agency is primarily responsible for interpreting the statute because the courts must defer to any reasonable construction it adopts. Courts appear to apply a more stringent standard of notice to civil regulations than civil statutes: parties are entitled to have 'ascertainable certainty' of what conduct is legally required by the regulation."[55]
3. ***Auer***: "where an agency interprets the meaning of its own regulation … courts typically must defer to the agency's reasonable interpretation" so "private parties are entitled to know with 'ascertainable certainty' an agency's interpretation of its regulation."[56]

The Third Circuit rejected Wyndham's invocation of the "ascertainable certainty" standard because it agreed with Wyndham's other argument: the court should analyze the meaning of Section 5 for itself under *Skidmore*:

---

[52] In re Lyca Tel, LLC, et al., *Dissenting Statement of Commissioner Michael O'Rielly*, File No. EB-TCD-12-00000403 (June 12, 2015), *available at* https://goo.gl/D5wF4Z.

[53] Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 250 (3rd Cir. 2015) (citing Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944)).

[54] *Id.* (citing CMR D.N. Corp. v. City of Phila., 703 F.3d 612, 631–32 (3d Cir. 2013)).

[55] *Id.* at 251 (citing Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984)).

[56] *Id.* at 251 (citing Auer v. Robbins, 519 U.S. 452, 461 (1997)).

> [I]f the federal courts are to decide whether Wyndham's conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply. The relevant question is not whether Wyndham had fair notice of the *FTC's interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires.[57]

Critical to this conclusion was Section 5(n), by which Congress, in 1994, codified the test at the heart of the FTC's 1980 Unfairness Policy Statement:

> In this context, the relevant legal rule is not "so vague as to be 'no rule or standard at all.'" *CMR D.N. Corp*., 703 F.3d at 632 (quoting *Boutilier v. Immigration & Naturalization Serv.*, 387 U.S. 118, 123 (1967)). Subsection 45(n) asks whether "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." While far from precise, **this standard informs parties that the relevant inquiry here is a cost-benefit analysis**, *Pa. Funeral Dirs. Ass'n v. FTC*, 41 F.3d 81, 89–92 (3d Cir. 1992); *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 975 (D.C. Cir. 1985), that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity. We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. *Cf. Nash v. United States*, 229 U.S. 373, 377 (1913) ("[T]he law is full of instances where a man's fate depends on his estimating rightly, that is, as the jury subsequently estimates it, some matter of degree."). Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.[58]

[57] *Id.* at 253–54.

[58] *Id*. at 255–56.

C. What this Means for the FTC

What does this mean for the FCC in how it might enforce Section 201(b) or Section 222(a) directly, on a case-by-case basis?

While Section 5(a) uses the words "unfair and deceptive," Congress gave greater specificity to unfairness through Section 5(n)'s three-part balancing test. By contrast, Section 201(b)'s vague standard is written at essentially the same level of conceptual generality as Section 5(a): "All … practices ... shall be just and reasonable." In other words, the FTC and Congress have developed a balancing test to give effect to the standard of 5(a), while the FCC has not yet done so in the same way for 201(b). Section 222(a) includes no balancing test at all: "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information."[59] The FCC's broader discretion under these provisions of Title II means, under the analysis of the *Wyndham* court, that the FCC will face a heightened burden in providing fair notice to regulated parties. It may also mean that the FCC cannot impose monetary penalties in pure case-by-case enforcement. On the other hand, the FCC's situation is significantly different from the FTC's in that it is dealing with far more sophisticated companies. Even though some of these may be small broadband providers, all at least know they are subject to the FCC's jurisdiction. By contrast, the FTC polices nearly every company in America, most of whom are unsophisticated and likely have no idea they are subject to the FTC's oversight on things like privacy and data security.

At a minimum, the FCC should better develop this thorny legal issue in a Further NPRM. In particular, the FCC should better summarize its past uses of Section 201(b) for both deception and unfairness.

IV. The FCC Should Harmonize Its Approach with the FTC

We urge the Commission to harmonize its substantive standards with those of the FTC — whether the Commission operates through case-by-case enforcement of Section 201(b) or 222(a) or through rulemaking. Specifically, we urge the FCC to adopt the careful balancing tests developed by the FTC, which have become the bedrocks of American consumer protection law — for privacy and data security just as much as for any other issue.

A. The FCC Should Follow the FTC's Deception Policy Statement

The FCC has already essentially adopted the FTC's 1983 Deception Policy Statement, via the Joint FCC/FTC Policy Statement For the Advertising of Dial-Around And Other Long-

[59] 47 U.S.C. § 222(a).

Distance Services To Consumers issued in 2000.[60] Most importantly, the FCC had already effectively adopted its own concept of materiality under Section 201(b):

> The FCC has taken a similar approach under section 201(b) of the Communications Act: "BDP knew, or should have known, that customers acting reasonably under the circumstances would be misled and confused by misrepresentations regarding the material issue of BDP's identity, and that customers would rely on such misrepresentations to their detriment."[61]

We urge the FCC to reaffirm that it will apply the FTC's Deception Policy Statement. To the extent that the FCC operates as the FTC has increasingly done in tech-related enforcement actions, relying on settlements rather than adjudication, we urge the Commission to take the materiality requirement seriously. Materiality serves an evidentiary proxy for injury — which, in turn, focuses enforcement on conduct that truly harms consumers:

> [T]he representation, omission, or practice must be a "material" one. The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception. **In many instances, materiality, and hence injury, can be presumed from the nature of the practice. In other instances, evidence of materiality may be necessary**. Thus, the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment….[62]
>
> A finding of materiality is also a finding that injury is likely to exist because of the representation, omission, sales practice, or marketing technique. Injury to consumers can take many forms. **Injury exists if consumers would have chosen differently but for the deception**. **If different choices are likely, the claim is material, and injury is likely as**

[60] Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers, *Policy Statement*, File No. 00-72 (rel. Mar. 1, 2000), *available at* https://goo.gl/npWx9O.

[61] *Id.* at n.5 (citing Business Discount Plan, Inc., *Notice of Apparent Liability for Forfeiture*, 14 FCC Rcd 340, 356 (1998)).

[62] Letter from the FTC to the Committee on Energy & Commerce, appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984) ["Deception Policy Statement" or "DPS"], *available at* https://goo.gl/TY5Ldc (emphasis added).

> **well. Thus, injury and materiality are different names for the same concept**.[63]

The materiality requirement, in short, keeps the FTC's focus where it should be — on consumers.

B. Why Should the FCC Follow the FTC's Approach?

The case for the FTC's approach was made quite ably by Former FTC Commissioner and Chairman Jon Leibowitz (Commissioner 2004–09, Chairman 2009–13) and FTC General Counsel Jonathan Nuechterlein (2013–16), writing about this proceeding:

> The critical question is how the FCC will exercise its new privacy powers. In our view, the FCC should follow the same basic approach that the FTC has successfully developed and enforced since the dawn of the commercial Internet.
>
> The FTC is mainly an enforcement agency rather than a regulator. It goes after companies when they break their privacy commitments to consumers or take actions that cause consumers real harm. This enforcement-oriented approach has a proven track record of success. It is flexible and promotes high-tech innovation, but it has held hundreds of companies, large and small, accountable when they crossed the line.
>
> The FCC should hold ISPs to the same privacy standards to which the FTC successfully held them for many years — and to which the FTC still holds all other companies. We were disappointed, then, when the FCC recently proposed to subject ISPs to a detailed set of burdensome data-privacy rules with no precedent in the FTC's regime. These rules would severely restrict how ISPs may use consumer data. For example, they would prevent any ISP from offering its own branded home security system to its existing customers without their advance permission. The rules would further subject all ISPs — and ISPs alone — to unprecedented compliance costs and keep them from efficiently monetizing online data in the same way that Google and Facebook have long done, with astounding consumer benefits. Such restrictions would exert upward pressure on broadband

[63] *Id.* at 6 (emphasis added).

> prices and undercut the FCC's central mission of promoting broadband investment and adoption.[64]

Unfortunately, as TechFreedom explained in its recent joint report on FTC process reforms, co-authored with the International Center for Law and Economics, the FTC has effectively broken the logic of the materiality "shortcut" by extending a *second* set of presumptions: most notably, that all express statements are material. This presumption may make sense in the context of traditional marketing claims, but it breaks down with things like privacy policies and other non-marketing claims (e.g., online help pages) — situations where deceptive statements certainly *may* alter consumer behavior, but in which such an effect cannot be presumed (because the company making the claim may not be doing so in order to convince consumers to purchase the product).[65] It is especially important that the FCC not presume that all express statements are material insofar as the FCC itself is requiring companies to make such statements via the Open Internet Order's transparency rule, which was the basis for the Commission's enforcement action against Verizon over supercookies.[66]

We do not say that misstatements in privacy policies cannot be material, only that the FCC cannot *presume* that they are material. It must establish materiality. Far from being a revision to the Deception Policy Statement, we believe this is what the FTC itself intended in this paragraph:

> The Commission considers certain categories of information presumptively material. First, the Commission presumes that express claims are material. As the Supreme Court stated recently [in *Central Hudson Gas & Electric Co. v. PSC*], "[i]n the absence of factors that would distort the decision to advertise, we may assume that the willingness of a business to promote

---

[64] Jon Leibowitz & Jonathan Nuechterlein, *The New Privacy Cop Patrolling the Internet*, FORTUNE (May 10, 2016), *available at* http://goo.gl/0qrZOB.

[65] *See* at Berin Szóka & Geoffrey Manne, *The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature: An Analysis of Proposed Legislation*, FTC: TECHNOLOGY & REFORM PROJECT: REPORT 2.0, at 21–26 ["FTC Reform Report"], *available at* http://goo.gl/36K7hM. Of course, even in the marketing context this presumption is one of administrative economy, not descriptive reality. While there is surely a correlation between statements intended to change consumer behavior and actual changes in consumer behavior, a causal assumption is not warranted. *See generally* Geoffrey A. Manne & E. Marcellus Williamson, *Hot Docs vs. Cold Economics: The Use and Misuse of Business Documents in Antitrust Enforcement and Adjudication*, 47 ARIZ. L. REV. 609 (2005).

[66] *Verizon Order*, *supra* note 17.

> its products reflects a belief that consumers are interested in the advertising."[67]

In effect, the first two sentences have come to swallow the rest of the paragraph, including the logic of the Supreme Court's decision in *Central Hudson,* the single most important case of all time regarding the regulation of commercial speech.[68] In particular, the FTC ignores the "absence of factors that would distort the decision to advertise."[69]

The FCC should not make the same mistake.

C. The FCC Should Follow the FTC's Unfairness Policy Statement

Even more important than following the FTC's 1983 Deception Policy Statement is following the FTC's 1980 Unfairness Policy Statement. The FCC appears to be reading both Section 201(b) and 222(a) to imply a kind of unfairness power, but has yet to articulate any limiting principles. Thus, we believe the FCC is in a situation essentially similar to that of the FTC in 1980 — prior to the adoption of the Unfairness or Deception Policy Statements, and to Congress's codification of the heart of the Unfairness Policy Statement in Section 5(n) in 1994, which reads as follows:

> The Commission shall have no authority under [Section 5(a)] to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice [(1)] causes or is likely to cause substantial injury to consumers [(2)] which is not reasonably avoidable by consumers themselves and [(3)] not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[70]

We urge the FCC to adopt this, but also the entirety of the Policy Statement by reference. The most relevant part bears reprinting here (minus the footnotes):

> First of all, the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into

[67] *Id.* at 5 (internal citations omitted).

[68] Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of NY, 447 U.S. 557 (1980).

[69] *Id.* at 567–68.

[70] 15 U.S.C. § 45(n).

purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction. [14] Unwarranted health and safety risks may also support a finding of unfairness.[15] Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair. Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers, as has been suggested in some of the comments.

Second, the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces. Most business practices entail a mixture of economic and other costs and benefits for purchasers. A seller's failure to present complex technical data on his product may lessen a consumer's ability to choose, for example, but may also reduce the initial price he must pay for the article. The Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects. The Commission also takes account of the various costs that a remedy would entail. These include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters. Finally, the injury must be one which consumers could not reasonably have avoided. Normally we expect the marketplace to be self-correcting, and we rely on consumer choice-the ability of individual consumers to make their own private purchasing decisions without regulatory intervention--to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.

> Sellers may adopt a number of practices that unjustifiably hinder such free market decisions. Some may withhold or fail to generate critical price or performance data, for example, leaving buyers with insufficient information for informed comparisons. Some may engage in overt coercion, as by dismantling a home appliance for "inspection" and refusing to reassemble it until a service contract is signed. And some may exercise undue influence over highly susceptible classes of purchasers, as by promoting fraudulent "cures" to seriously ill cancer patients. Each of these practices undermines an essential precondition to a free and informed consumer transaction, and, in turn, to a well-functioning market. Each of them is therefore properly banned as an unfair practice under the FTC Act.[71]

This balancing test ensures that the FTC is focused on practices that actually harm consumers, which ensures that the agency prioritizes its limited enforcement resources properly, and avoids proscribing conduct that actually benefits consumers. This test would serve the FCC equally well.

D. The FCC Should Adopt the Substantive Test of Section 5 If It Issues Rules

We are not necessarily opposed to a rulemaking on broadband privacy, especially if that rulemaking more generally incorporates standards of reasonableness such as the FCC has proposed in 47 C.F.R. § 64.7005 ("A BIAS provider may employ any security measures that allow the provider to *reasonably* implement the requirements set forth in this section").[72] Again, a rulemaking *may* be the best way to provide fair notice of what the FCC will require in subsequent enforcement, especially insofar as that enforcement involves monetary penalties.

But any FCC privacy or data-security rulemaking should be firmly grounded in the substantive standards that have guided the FTC's case-by-case enforcement on privacy and data security — just as an FTC rulemaking under Section 5 would be.

This is not a novel situation. Although the FTC has given up using its Section 5 rulemaking powers in favor of operating purely through case-by-case enforcement and now conducts rulemakings only pursuant to narrow issue-specific grants of authority, for which Congress

---

[71] Letter from Michael Pertschuk, Chairman, FTC, to Hon. Wendell H. Ford, Chairman, Senate Comm. on Commerce, Science, and Transportation (Dec. 17, 2980), appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984), *available at* https://goo.gl/TVjZI4.

[72] NPRM ¶¶ 109–10.

has given it authority to issue rules under the Administrative Procedure Act (rather than under the heightened evidentiary standards and procedural safeguards for rulemakings under Section 5), the FTC still looks to Section 5 to guide these rulemakings. For instance, in a2015 dissent from the FTC's vote to update the Telemarketing Sales Rule to ban telemarketers from using four "novel" payment methods, Commissioner Ohlhausen chided the FTC for not developing an adequate evidentiary record to satisfy the cost-benefit test of Section 5(n). She cited no less an authority than the Federal Reserve Bank of Atlanta (FRBA), which is not merely one of twelve Federal Reserve Branches, but the one responsible for "operat[ing] the Federal Reserve System's Retail Payments Product Office, which manages and oversees the check and Automated Clearing House (ACH) services that the Federal Reserve banks provide to U.S. financial institutions."[73] Ohlhausen explained:

> The amendments do not satisfy the third prong of the unfairness analysis in Section 5(n) of the FTC Act, which requires us to balance consumer injury against countervailing benefits to consumers or competition. Although the record shows there is consumer injury from the use of novel payment methods in telemarketing fraud, it is not clear that this injury likely outweighs the countervailing benefits to consumers and competition of permitting novel payments methods….
>
> In sum, the FRBA's analysis of the prohibition of novel payments in telemarketing indicates that any reduction in consumer harm from telemarketing fraud is outweighed by the likely benefits to consumers and competition of avoiding a fragmented law of payments, not limiting the use of novel payments prematurely, and allowing financial regulators working with industry to develop better consumer protections.[74]

In short, the FTC majority failed to undertake an economically rigorous analysis of the sort the Commission's Bureau of Economics would likely perform, in this case failing to properly weigh injury against countervailing benefits as Section 5(n) requires. At a minimum, the FTC would have done well to solicit further public comment on its rule, heeding the experience of past chairmen, as summarized by Former Chairman Tim Muris:

> By their nature, however, rules also must apply to legitimate actors, who actually deliver the goods and services they promise. Remedies and ap-

[73] In the Matter of the Telemarketing Sales Rule, *Separate Statement of Commissioner Maureen K. Ohlhausen, Dissenting in Part*, Project No. R411001, at n.3 (Nov. 18, 2015), *available at* https://goo.gl/KnY1W0.

[74] *Id*. at 1–2.

> proaches that are entirely appropriate for bad actors can be extremely burdensome when applied to legitimate businesses, and there is usually no easy or straightforward way to limit a rule to fraud. Rather than enhancing consumer welfare, overly burdensome rules can harm the very market processes that serve consumers' interests. For example, the Commission's initial proposal for the Telemarketing Sales Rule was extremely broad and burdensome, and one of the first acts of the Pitofsky Commission was to narrow the rule. More recently, the Commission found it necessary to re-propose its Business Opportunity Rule, because the initial proposal would have adversely affected millions of self-employed workers.[75]

This precisely is the kind of mistake the FCC should avoid in this rulemaking. It should more carefully weigh the economic tradeoffs involved in imposing new privacy and data security regulations on broadband providers — especially given that (a) the conduct at issue is not fraud or some other form of inherently harmful conduct, but a question of striking the proper balance in how much data security is enough, how to balance the benefits of data use with its potential costs, and so on and (b) that the FCC is crafting rules that will uniquely burden one set of companies in the Internet ecosystem (i.e., broadband providers) while the rest (i.e., edge providers) continue to operate under the FTC's more flexible, case-by-case approach.

Finally, it is worth remembering that the cost-benefit test implicit in unfairness and the materiality requirement in deception are only half of the process developed in the back and forth between the FTC and Congress that reached its dramatic climax in 1980. The other half are the heightened evidentiary burden and procedural safeguards Congress imposed upon the FTC for Section 5 rulemakings in early 1980. We believe these remain sensible safeguards, amply justifiable for any rulemaking conducted under a standard that is as broad and vague as Section 5 of the FTC Act — or, for that matter, Section 201(b) of the Communications Act. Of course, the FCC is not subject to those requirements, and embracing the FTC's *substantive* standards would not *require* the FCC to follow the same *procedural* standards. Nonetheless, we believe the FCC would do well to consider these requirements and implement their spirit. At a minimum, that would require the Commission to distill the feedback received in this comment round into a Further NPRM that includes

---

[75] Statement of Timothy J. Muris, Hearing on Financial Services and Products: The Role of the Fed. Trade Commission in Protecting Customers, before the Subcomm. on Consumer Protection, Prouct Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation, 111th Cong. 2nd Session, at 24 (2010), *available at* http://goo.gl/gbejB1.

meaningful analysis of how broadband providers currently use, process and store data, and might do so in the future, informed both by economists and technical experts. There is too much at stake here for this rulemaking to be yet another "economics-free zone," as the FCC's "net neutrality" rulemaking was.[76]

E. The FCC Incorrectly Cites the FTC's Big Data Report on Discounts

We also note that the FCC's NPRM cites the FTC comments regarding findings about what the FCC labels as "financial inducement practices," more commonly known to consumers as "discounts." But the concerns expressed in that report, as cited by the NPRM, came not from the FTC staff, but rather from participants in the FTC's workshop on big data. Any rule on "financial inducement practices" should reflect the FTC report's countervailing caution that ". . .choice options may result in lower prices or other consumer benefits, as companies develop new and competing ways of monetizing their business models."[77] This apparent disconnect, in addition to all the foregoing reasons already discussed, gives added reason for the FCC to issue a FNPRM in this proceeding.

V. Section 705 of the Communications Act Actually *Curtails* the FCC's Authority.

The FCC also cites Section 705 of the Communications Act[78] as a source of authority for its proposal.[79] But this provision cannot support the NPRM, as Section 705 actually *curtails* the Commission's authority to regulate the interception of communications by broadband providers. And to the extent that the proposed rules would dictate the circumstances in which broadband providers can access and use the contents of their subscribers' communications, they conflict with Congress's deliberate decision to place the Wiretap Act's core provisions *outside* of the statute the Commission is authorized to administer. In any event, at most, Section 705 would support only limited privacy rules and only for mobile broadband.

---

[76] Tim Brennan, *Is the Open Internet Order an "Economics-Free Zone"?*, PERSPECTIVES FROM FSF SCHOLARS (June 28, 2016), *available at* http://goo.gl/WAju6c.

[77] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Comments of FTC Commissioner Maureen K Ohlhausen*, at 4 (May 27, 2016), *available at* https://goo.gl/jp6dQ2.

[78] 47 U.S.C. § 605.

[79] NPRM ¶ 307.

A. After Enacting Section 705 in 1934, Congress Narrowed It in 1968

Section 605 of the Communications Act of 1934[80] — which was later renumbered as Section 705 of the Act[81] — originally prohibited the following:

1. Divulging or publishing, without authorization, the contents of a private "interstate or foreign communication by wire or radio" by any person involved in transmitting or receiving the communication, except in limited circumstances;[82]
2. Intercepting and divulging the contents of a private "interstate or foreign communication by wire or radio" by any person not authorized by the sender to do so;[83]
3. Receiving a private "interstate or foreign communication by wire or radio" without authorization, and using the contents of the communication to benefit any person not entitled thereto;[84] or
4. Having received a private "interstate or foreign communication by wire or radio," or the contents thereof, and knowing that it was intercepted without authorization, divulging or publishing the contents of the communications or using them to the benefit of any person not entitled thereto.[85]

In 1968, Congress significantly revised this provision by passing the Omnibus Crime Control and Safe Streets Act — the third title of which is commonly known as the Wiretap Act — to provide a more comprehensive legal framework regarding the interception of communications.[86] The Wiretap Act placed this framework in a new chapter of Title 18 of the U.S. Code,[87] while also amending Section 705 of the Communications Act by considerably narrowing its scope.[88] As originally enacted in 1934, each prohibition in Section 705 encompassed "interstate or foreign communication *by wire or radio*."[89] However, the Wiretap

---

[80] Communications Act of 1934, Pub. L. No. 73-415, § 605, 48 Stat. 1064, 1103 (1934).

[81] Cable Communications Policy Act of 1984, Pub. L. No. 98–549, § 6(a), 98 Stat. 2779, 2804 (1984).

[82] 47 U.S.C. § 605(a) (excepting, *inter alia*, the divulging of contents to "the addressee, his agent, or his attorney"; "to a person employed or authorized to forward such communication to its destination"; to "proper accounting or distributing officers of the various communicating centers over which the communication may be passed"; "to the master of a ship under whom he is serving," or "in response to a subpena [sic] issued by a court of competent jurisdiction, or on demand of other lawful authority").

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–22).

[87] *See* 18 U.S.C. §§ 2510–2522 (chapter 119).

[88] Pub. L. No. 90-351, § 803, 82 Stat. 197, 223.

[89] Pub. L. No. 73-415, § 605, 48 Stat. 1064, 1103 (emphasis added); *see also supra* notes 80–85 and accompanying text.

Act narrowed Section 705 such that only its first clause — which prohibits any person involved in the receipt or transmission of a communication from divulging or publishing the contents thereof — applied to *both* wire and radio communications.[90] As for all the other prohibitions in Section 705, the Wiretap Act limited their applicability to "radio communications."[91] At the same time, the Wiretap Act added a series of new provisions — codified as amended at Sections 2510 to 2522 of Title 18, U.S. Code — which set forth the penalties for intercepting without authorization any "wire, oral, or electronic communication"[92] and provided a legal framework by which law enforcement entities may seek a court order to intercept such communications.[93] In other words, the Wiretap Act provisions in Title 18 address the interception of communications *other than radio communications*, whereas Section 705 addresses the interception of radio communications.

This change reflects Congress's decision to place the bulk of statutory restrictions on wiretapping *beyond* the FCC's ambit, leaving inside the Communications Act only a modest portion of the overall 1934 scheme governing the interception of communications. From this, it seems clear that Congress intended for Section 705 to be applied in a manner consistent with the other Wiretap Act provisions, as it indicated by prefacing the prohibitions in Section 705 with the phrase "[e]xcept as authorized by chapter 119, title 18"[94] — in other words, "except as authorized by [the Wiretap Act]."[95] Although this phrase appears only once in Section 705, the U.S. Court of Appeals for the Fifth Circuit has held that it "limits each of [Section 705's] prohibitions to activities not authorized by the Wiretap Act."[96] "Since Congress added the introductory phrase to [Section 705] at the same time that it enacted the Wiretap Act," the Fifth Circuit wrote, "we believe Congress likely intended to

[90] Pub. L. No. 90-351, § 803, 82 Stat. 197, 223.

[91] *Id.*

[92] *See* 18 U.S.C. § 2511(1)(a). This provision originally covered only "wire or oral communication" but was amended in 1986 to also include "electronic" communications. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(c)(1)(A), 100 Stat. 1848, 1851 (1986).

[93] *See* 18 U.S.C. §§ 2516–18.

[94] 47 U.S.C. § 605(a).

[95] The Fifth Circuit used this modified version of the phrase interchangeably with the statutory text in Edwards v. State Farm Ins. Co., 833 F.2d 535, 539 (5th Cir. 1987).

[96] *Id.* at 540.

make the statutes consistent."[97] And, importantly, the Wiretap Act is administered by the courts — not by the FCC.[98]

Although the NPRM briefly acknowledges the legislative history of Section 705's prohibitions in a footnote, it does not even attempt to analyze how Congress's 1968 amendment to the provision might affect the FCC's authority to issue rules based on Section 705.[99] Nor does the NPRM cite a single judicial opinion interpreting the Wiretap Act's exceptions, despite the fact that numerous courts have examined the comprehensive scheme Congress enacted therein to govern the interception of wire, oral, electronic, and radio communications.[100] Perhaps the FCC prefers to downplay such constraints on its authority that come from outside of the statute it is empowered to administer — but as federal appellate courts have made clear, an agency that ignores such constraints does so at its own peril.[101]

B. The Wiretap Act Allows Broadband Providers to Intercept the Communications of Subscribers Who Have Given Their Consent

Had the FCC conducted even a half-hearted analysis of the Wiretap Act, it would have noted that the statute permits a person "not acting under color of law to intercept a wire, oral, or electronic communication … where one of the parties to the communication has given *prior consent* to such interception."[102] The Act also states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication … with the *lawful consent* of the originator or any addressee or intended recipient of such communication."[103] And the Act allows "a provider of … electronic communication service, whose facilities are used in the transmission of … electronic communication, to intercept, disclose, or use that communication … while engaged in any activity which is a

---

[97] *Id.*

[98] *Cf.* Crandon v. United States, 494 U.S. 152, 177 (1990) (Scalia, J., concurring) (declining to defer to administrative interpretations of 18 U.S.C. § 209(a), noting that, as a "criminal statute," it "is not administered by any agency but by the courts").

[99] NPRM, 31 FCC Rcd at 2597, ¶ 307 n.477.

[100] The NPRM contains a handful of cursory citations to the Wiretap Act, none of which actually discuss how it limits the ability of broadband providers to intercept subscriber communications. *See, e.g.*, NPRM, 31 FCC Rcd at 2523, ¶ 67 nn.122–23; *id.* at 2549, ¶ 137 n.247; *id.* at 2597, ¶ 307 n.477.

[101] *See, e.g.*, Adams Fruit Co. v. Barrett, 494 U.S. 638, 650 (1990) ("[A]n agency may not bootstrap itself into an area in which it has no jurisdiction.") (citing Federal Maritime Comm'n v. Seatrain Lines, Inc., 411 U.S. 726, 745 (1978)).

[102] 18 U.S.C. § 2511(2)(d) (emphasis added).

[103] 18 U.S.C. § 2511(3)(b)(ii) (emphasis added).

necessary incident to the rendition of … service or to the protection of the rights or property of the provider."[104]

A broadband provider is an "electronic communications service" provider within the meaning of the Wiretap Act.[105] As such, a broadband provider may intercept a subscriber's Internet communications, or divulge them to a person who is not a party to the communications, if and only if the provider has satisfied one of the Wiretap Act's exemptions. In the context of this NPRM, which purports to regulate how providers may use and disclose "customer PI" for marketing and other purposes unnecessary to furnishing the underlying service,[106] the consent exemption is key. The NPRM addresses consent in its proposed definitions of "opt-out" and "opt-in" approval,[107] but ignores Congress's decision to align the Communications Act with the Wiretap Act's provisions governing the interception of the contents of communications.[108] Simply put, the FCC lacks the authority to regulate a broadband provider's interception of Internet traffic where such interception is expressly permitted by the Wiretap Act.[109]

What does it mean for a broadband customer to "consent" to the interception of her traffic by her provider? Simply put, a customer consents when she expressly or implicitly manifests her assent to such interception. This manifestation may occur in a variety of ways: "In the [the Wiretap Act] milieu as in other settings, consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights."[110] In general, "consent must be express,"[111] although it may also be implied by "surrounding circumstances"[112] — but, in either case, consent "must be actual."[113] Thus,

---

[104] 18 U.S.C. § 2511(2)(a).

[105] "Traffic on the Internet is electronic communication." Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1246 (10th Cir. 2012) (applying 18 U.S.C. § 2511(1) to a broadband provider).

[106] *See, e.g.*, NPRM, 31 FCC Rcd at 3606 (proposing 47 C.F.R. § 64.7002(a), which lists the purposes for which a BIAS provider's customer is presumed to have granted approval by virtue of using the service).

[107] NPRM, 31 FCC Rcd at 2523–22, ¶¶ 68–70.

[108] *See supra* notes 95–99.

[109] "Regardless of how serious the problem an administrative agency seeks to address, … it may not exercise its authority in a manner that is inconsistent with the administrative structure that Congress enacted into law." Verizon v. FCC, 740 F.3d 623, 634 (D.C. Cir. 2014) (quoting Ragsdale v. Wolverine World Wide, Inc., 535 U.S. 81, 91 (2002)) (internal quotation marks omitted).

[110] Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990).

[111] United States v. Staves, 383 F.3d 977, 981 (9th Cir. 2004).

[112] *Id.*

[113] Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014) (citing United States v. Van Poyck, 77 F.3d 285, 292 (9th Cir. 1996), United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987), and United States v. Corona-Chavez, 328 F.3d 974, 978 (8th Cir. 2003)).

if a person signs a form acknowledging that another entity will monitor her communications, her consent will suffice to exempt that entity from Wiretap Act liability.[114] According to the U.S. Court of Appeals for the Second Circuit, "[t]he legislative history [of the Wiretap Act] shows that Congress intended the consent requirement to be construed broadly."[115] In the case of Internet services, courts have held that a provider's terms of service are sufficient to establish consent if the terms "adequately notif[y] the reasonable" user of the interception.[116] In contrast, a provider's terms of service do not provide adequate notice where the disclosure of interception is "buried in a Terms of Service or Privacy Policy that may never be viewed or if viewed at all on a wholly separate page disconnected from the processes that led to" the interception of a user's communications.[117]

Thus, at most, the FCC may be able to invoke Section 705 to regulate the adequacy of notice provided by mobile broadband providers to their customers governing how their data may be collected ("intercepted"[118]) and shared with third parties ("divulged"[119]). But the FCC may *not* require use Section 705 to mandate anything beyond what Congress required under the Wiretap Act, including how data may be used internally once consent has been obtained, data-security practices, and data-breach notification.

C. The Proposed Rules Conflict with the Wiretap Act Insofar as They Regulate Broadband Providers' Interception of Content

The NPRM skirts the issue of whether broadband providers may intercept the contents of their subscribers' communications, what consent this might require, or for what purposes intercepted content may be used. Instead, the NPRM asks only broadly for "comment on how" the FCC "should define and treat the content of customer communications."[120] It also asks "whether the use of DPI" — i.e., deep packet inspection[121] — "for purposes other than

---

[114] *See, e.g.*, United States v. Hammond, 148 F. Supp. 2d 589, 591 (D. Md. 2001), *aff'd*, 286 F.3d 189 (4th Cir. 2002).

[115] United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987).

[116] In re Yahoo Mail Litigation, 7 F. Supp. 3d 1016, 1029 (N.D. Cal. 2014) (holding that Yahoo's terms of service established that Yahoo Mail users had given "explicit consent" to Yahoo scanning and analyzing their email for various purposes, including targeting advertising).

[117] Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014).

[118] 18 U.S.C. § 2511(2)(c) & (d).

[119] 18 U.S.C. § 2511(3)(b).

[120] NPRM, 31 FCC Rcd at 2523, ¶ 67.

[121] As the NPRM explains, "DPI involves analyzing Internet traffic beyond the basic header information necessary to route a data packet over the Internet. DPI is used by network operators to gather information about the contents of a particular data packet, and may be used for reasonable network management, such as some tailored network security practices. In addition, DPI has been used by network providers in order to serve

providing broadband services, and reasonable management thereof, should be prohibited or otherwise subject to a heightened approval framework."[122] And the NPRM "seek[s] comment on whether [the Commission] should consider application headers CPNI in the broadband context."[123] Based on these inquires, a reader might interpret the NPRM as an indication that the FCC has not yet decided to regulate when broadband providers may use or divulge the *contents* of their subscribers' communications.

Yet the proposed rules themselves make no distinction between basic subscriber information, metadata, and the contents of subscriber communications. The NPRM's requirements would apply whenever a broadband provider wishes to "use, disclose, or provide access to customer PI."[124] Customer PI, or "Customer Proprietary Information," is defined as "(1) Customer proprietary network information; and (2) Personally identifiable information (PII) a BIAS provider acquires in connection to its provision of BIAS."[125] And "personally identifiable information" (PII) is defined as "any information that is linked or linkable to an individual."[126] Although the rules themselves do not elaborate on the definition of PII, the NPRM proposes that "types of PII include … eponymous and non-eponymous online identities; … Internet browsing history; … application usage data; … shopping records; medical and health information," among many others.[127]

In other words, under the proposed rules, if a provider acquires information about a subscriber's web-browsing habits in the course of providing Internet access, and it wishes to use that information to deliver targeted advertisements to that subscriber for non-communication-related services, the provider must first "solicit customer approval"[128] pursuant to opt-in requirements outlined in the NPRM.[129] The rules make no distinction between a provider's acquisition of customer PI by accessing non-content metadata, such as Internet Protocol packet headers,[130] and the acquisition of such information by intercept-

---

targeted advertisements. DPI has also been used by network providers to identify and block specific packets." *Id*. at 2584, ¶ 264 & nn.411–14.

[122] *Id.* at 2584–85, ¶¶ 264–67.

[123] *Id.* at 2517–18, ¶ 50.

[124] *Id.* at 2606 (proposing 47 C.F.R. § 64.7002).

[125] *Id.* at 2604 (proposing 47 C.F.R. § 64.7000(f)).

[126] *Id.* at 2604 (proposing 47 C.F.R. § 64.7000(j)).

[127] *Id.* at 2521–22, ¶ 62.

[128] *See id.* at 2607(proposing 47 C.F.R. § 64.7002(c)).

[129] *Id.* at 2607(proposing 47 C.F.R. § 64.7002(f)).

[130] *Cf. id.* at 2516, ¶ 45 ("We propose to consider both source and destination IP addresses as CPNI in the broadband context."); *see also* Protecting the Privacy of Customers of Broadband and Other Telecommunica-

ing packets and inspecting their payload for uniform resources locators (URLs), also known as web addresses.[131] If the Commission does not intend to restrict when providers may intercept and use the contents of subscriber communications, why do the proposed rules lack an exemption or other language clarifying that they apply only to a provider's use of information *other than* the contents of such communications?

It appears this is because the FCC is, in fact, seeking to regulate how providers may use the contents of their subscribers' communications — thus contravening the Wiretap Act's limitations on the agency's authority. In a paragraph requesting comment on whether "application headers" should be considered CPNI, the NPRM includes a footnote that states:

> Requested URLs may contain particularly detailed information about the type, form, and *content* of a communication between a user and a website. For instance, query strings within a URL may indicate the *contents* of a user's search query, the *contents* of a web form, or other information.[132]

The FCC thus recognizes that an application header may contain the "content of a communication," but it nonetheless asks whether such information should be treated as CPNI.[133] Moreover, regardless of how this inquiry is ultimately resolved, the text of the rules as proposed plainly encompasses application headers, even if the Commission does not realize it.[134] In short, the FCC is proposing to regulate how providers use the contents of their subscribers' communications, while treating the Wiretap Act as less than an afterthought.

Even if, contrary to our analysis above, Congress had empowered the FCC to resolve ambiguities in the Wiretap Act, several courts have already addressed the question of whether intercepting URLs meets the statutory definition of "intercept," which "means the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[135] Their conclusion: URLs can be content.[136] Thus, any attempt by the FCC to use Section 705 to regulate URLs and other packet-

---

tions Services, *Comments of the Center for Democracy & Technology*, at 12–16 (May 27, 2016), *available at* https://goo.gl/UwaoWi (arguing that customer PI must include packet metadata).

[131] *Cf.* NPRM at 2517–18, ¶ 50.

[132] *Id.* at 2517 n.81 (emphases added) (citing Andrew G. West & Adam J. Aviv, *On the Privacy Concerns of URL Query Strings*, 2014 Proc. of the 8th Workshop on Web 2.0 Sec. and Privacy (2014), *available at* http://goo.gl/3bDsDJ).

[133] NPRM, 31 FCC Rcd at 2517–18, ¶ 50.

[134] *See supra* notes 124–131 and accompanying text.

[135] 18 U.S.C. § 2510(4) (emphasis added).

[136] *See* In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 139 (3d Cir. 2015) ("[R]outing information and content are not mutually exclusive categories. And between the information re-

header metadata — which could be content — as CPNI, beyond the scope authorized by the Wiretap Act, would be unlawful.

Moreover, even under an extremely generous interpretation of Section 705, Congress's decision[137] in 1968 to exclude *non-radio* communications from every clause in the section other than its first clause — which, again, addresses only who may divulge or publish of the contents of communications — means that the Commission's authority to regulate the interception of contents cannot extend to *wireline* providers of electronic communications.[138] Yet the FCC ignores this distinction in its NPRM, proposing to regulate the privacy practices of wireless and wireline broadband providers alike.[139] The Commission may feel emboldened by the recent D.C. Circuit panel opinion in *U.S. Telecom Association v. FCC* deferring to the agency's finding that mobile broadband is a telecommunications service under Title II of the Communications Act,[140] but this opinion does not give the FCC carte blanche to treat wireline and wireless broadband services as interchangeable.

VI. Section 706 of the Telecom Act Is Not an Independent Grant of Regulatory Authority.

Unsurprisingly, the Commission decided to once again include Section 706 of the Telecommunications Act of 1996 in its legal-authority grab bag.[141] We have long argued, both at the FCC[142] and in court,[143] that Section 706 cannot reasonably be interpreted to confer in-

---

vealed by highly detailed URLs and their functional parallels to post-cut-through digits, we are persuaded that — at a minimum — some queried URLs qualify as content.) (citing Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1030 n.93 (2010)); Redacted Foreign Intelligence Surveillance Court Memorandum Opinion, PR/TT, *available at* https://goo.gl/JPyldQ; *see also* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000) (vacating FCC order requiring carriers covered by CALEA to provide "all dialed digits pursuant to a pen register order" — including all post-cut-through digits — and suggesting that a "Title III warrant" might be required to receive such information).

[137] Pub. L. No. 90-351, § 803, 82 Stat. 197, 223.

[138] *See supra* notes 87–93 and accompanying text.

[139] NPRM, 30 FCC Rcd at 2613–16, ¶¶ 8–18 (Appendix B).

[140] U.S. Telecom Ass'n v. FCC, No. 15-1063, slip op. at 55 (D.C. Cir. June 14, 2016).

[141] 47 U.S.C. § 1302; NPRM ¶¶ 308–09.

[142] *See, e.g.*, Protecting and Promoting the Open Internet, *Legal Comments of TechFreedom & ICLE*, GN Docket No. 14-28, at 62–91 (July 17, 2014), *available at* http://goo.gl/ZgVn6n; Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act, *Reply Comments of TechFreedom & ICLE*, GN Docket No. 14-126, at 15–21 (Apr. 6, 2015), *available at* http://goo.gl/3uVhYQ.

[143] Brief for Scholars of Law & Economics et al. as Amici Curiae Supporting Petitioners, Tennessee v. FCC, No. 15-3291, at 10–31 (6th Cir. Sept. 25, 2015), *available at* http://goo.gl/v1WFLi.

dependent regulatory authority upon the FCC. While it may have played a key role in the Senate's vision of "AN END TO REGULATION,"[144] and thus reasonably have been characterized as "a necessary fail-safe" in the Senate committee's report,[145] such language was not included in the report of the conference committee that fused the House and Senate versions of the would-be Telecom Act.[146]

All of the tools Congress included by specific mention in Section 706 — and all the measures the conference committee said were authorized under Section 706 — were already granted to the Commission in the Communications Act. The full text of the conference committee's discussion indicates as much:

> **SECTION 706 — ADVANCED TELECOMMUNICATIONS INCENTIVES**
>
> **Senate bill**
>
> Section 304 of the Senate bill ensures that advanced telecommunications capability is promptly deployed by requiring the Commission to initiate and complete regular inquiries to determine whether advanced telecommunications capability, particularly to schools and classrooms, is being deployed in a ''reasonable and timely fashion.'' Such determinations shall include an assessment by the Commission of the availability, at reasonable cost, of equipment needed to deliver advanced broadband capability. If the Commission makes a negative determination, it is required to take immediate action to accelerate deployment. Measures to be used include: price cap regulation, regulatory forbearance, and other methods that remove barriers and provide the proper incentives for infrastructure investment. The Commission may preempt State commissions if they fail to act to ensure reasonable and timely access.
>
> **House amendment**
>
> No provision.
>
> **Conference agreement**

[144] S. 652 ES, 104th Cong., 2 (June 15, 1995) (Engrossed in Senate), *available at* https://goo.gl/XBgXUG.

[145] *See* S. Rep. No. 104-23, at 51 (Mar. 30, 1995), *available at* https://goo.gl/CJt6TS; *see also* Verizon v. FCC, 740 F.3d 623, 639 (D.C. Cir. 2014).

[146] Conf. Rep. No. 104-458, at 210 (Jan. 31, 1996), *available at* https://goo.gl/V5B559.

> The conference agreement adopts the Senate provision with a modification.[147]

The non-exhaustive list of measures the FCC is directed to use in response to a negative finding under Section 706(b) are all tools specifically granted to the FCC in the Communications Act. "[P]rice cap regulation,"[148] "regulatory forbearance,"[149] and "other methods that remove barriers … [to] infrastructure investment[,]" including preemption,[150] are already in the FCC's toolkit. And while the "include" language in Section 706 suggests that the list of measures is non-exhaustive, the interpretive canon of *noscitur a sociis* (Latin for "it is known by its associates") suggests that the regulatory "measures" to be used by the Commission to "promote competition" and "remove barriers to infrastructure investment" are similar to the specific regulatory tools listed in the provision — i.e., tools already available to the FCC under the Communications Act.

Thus, Section 706 cannot reasonably be interpreted to confer independent regulatory authority upon the Commission. In light of commonly-accepted tools of statutory construction, including interpretive canons and legislative history, the Congressional intent behind Section 706 is clear. It is merely a policy statement (subsection (a)) and a bellwether (subsection (b)) Congress used to: (1) put a thumb on the scale, directing the FCC to do everything within its power to promote broadband deployment; and (2) regularly assess how broadband deployment is proceeding, in order to ascertain whether and when Congress should step in again to adopt broadband-specific legislation. As such, the FCC may point to Section 706 as support for using one of its other powers in such a way that promotes broadband competition and deployment, but it cannot do with Section 706 something it could not otherwise do with the Communications Act. Therefore, in the instant proceeding, the Commission may point to Section 706 for support in using one of its other authorizes — such as Section 222 — in such a way that promotes broadband, but it cannot base its proposed privacy and data-security rules on Section 706 alone.

---

[147] *Id.*

[148] *See* 47 U.S.C. § 203; *see also* Policies and Rules Concerning Rates for Dominant Carriers, *Second Report and Order*, 5 FCC Rcd. 6786 (rel. Oct. 4, 1990), *available at* https://goo.gl/6p04Re (extending price-cap regulations to ILECs).

[149] 47 U.S.C. § 160.

[150] 47 U.S.C. § 253.

While recent appellate court decisions offer some hope for the FCC in trying to use Section 706 as a standalone basis of authority,[151] we remain convinced that these decisions were in error.

The discussion of Section 706 by the Tenth Circuit panel of judges in *In re FCC 11-161* was exceedingly brief, encompassing a mere six pages in an opinion spanning 143 pages, and even much of that six pages consists of block quotes pulled directly from the FCC's order on review and Section 706 itself.[152] This scant analysis would deserve little weight even if it were necessary to the outcome of the case, and, since it was not — as the FCC's USF-ICC Transformation Order was upheld based on Section 254 — it is entirely unpersuasive and should be disregarded.

The *Verizon* court discussed Section 706 in greater detail, but, as in *In re FCC 11-161*, we believe none of that discussion was necessary to the holding of the case: The 2010 Open Internet Order's rules against blocking and unfair discrimination were thrown out for invalidly imposing common-carrier duties on non-common carriers,[153] while the transparency rule — the only rule to survive — was not being challenged (other than by Verizon saying it was not severable from the rest of the order, and should fall along with the rest) and, as noted by Judge Silberman in dissent, could have been upheld under the FCC's authority ancillary to Section 257.[154] Thus, we maintain that the discussion of Section 706 was not necessary to the outcome of the case, and therefore should not have been considered binding precedent by the D.C. Circuit panel of judges in *U.S. Telecom Ass'n v. FCC*.[155]

While the D.C. Circuit's discussion and analysis of Section 706 in *Verizon* was more fulsome than the 10th Circuit's, it still is not very persuasive, as the panel failed to consider a key element of *Chevron* in deciding whether to give deference to the FCC's interpretation: Agencies are entitled to deference in interpreting ambiguous provisions of their own statutes, but Section 706 — unlike its neighboring provisions in Title VII of the Telecommunications Act[156] — was not inserted into the Communications Act. Thus, while the court re-

---

[151] *See* U.S. Telecom Ass'n v. FCC, No. 15-1063, slip op. at 94–97 (D.C. Cir. June 14, 2016), *available at* https://goo.gl/Wt3T7q; Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014); In re FCC 11-161, 753 F.3d 1015 (10th Cir. 2014).

[152] *Id.* at 1049–54.

[153] Verizon v. FCC, 740 F.3d at 650–59.

[154] *Id.* at 668 n.9 (Silberman, J., dissenting).

[155] U.S. Telecom Ass'n v. FCC, *supra* note 8, at 96–97.

[156] *See* Telecommunications Act of 1996, Pub. L. 104-104, § 705, 110 Stat. 153 (1996) (codified at 47 U.S.C. § 332); Telecommunications Act of 1996, Pub. L. 104-104, § 707, 110 Stat. 154 (1996) (codified at 47 U.S.C. § 309).

jected the argument that Section 706 cannot be read to be an independent grant of authority because Congress does not "hide elephants in mouseholes[,]"[157] as Section 706 was not inserted into the Communications Act — the Act the FCC is tasked with administering and its principal source of statutory authority — it is more accurate to argue that Section 706 cannot be read to be an independent grant of authority because Congress also does not make mountains out of molehills, with the difference being that mouseholes are typically found indoors (i.e., inside the Communications Act) whereas molehills are typically found outdoors (i.e., outside the Communications Act). The *Verizon* court failed to consider this key line of argumentation, and therefore we believe its analysis of Section 706 — insofar as it carries weight even as dicta — should be discounted in weight accordingly.

In *U.S. Telecom Ass'n v. FCC*, Judges Tatel and Srinivasan accepted the *Verizon* analysis of Section 706, rejecting arguments that it was dicta and refusing to reengage in the statutory analysis by saying the court was bound by the *Verizon* precedent.[158] However, that aspect of the opinion may be overturned by the D.C. Circuit *en banc*, or by the Supreme Court, which will be particularly likely to take up the issue if the municipal broadband preemption case still pending before the Sixth Circuit comes down the opposite way on the question of what authority Section 706 grants to the Commission. We therefore encourage the Commission to avoid premising any of its proposed privacy or data-security rules on Section 706, lest the legal landscape change on this issue and cut the rules' authority out from under them.

Finally, even if Section 706 *were* held to be an independent source of regulatory authority for the FCC, the same line of reasoning presented above dictates that it could not be used as a basis on which to impose monetary penalties. The FCC's authority to impose monetary penalties comes from Section 503(b) of the Communications Act,[159] which specifically limits said authority to "Any person who is determined by the Commission … to have — willfully or repeatedly failed to comply with any of the provisions of this chapter or of any rule, regulation, or order issued by the Commission under this chapter[.]"[160] Since "this chapter" refers to the Communications Act, and since Section 706 was *not* inserted into the Communications Act, Section 503(b) cannot be used by the Commission to impose any monetary penalties pursuant to Section 706. Thus, at most, the Commission could use Section 706 on-

[157] Verizon v. FCC, 740 F.3d at 639.

[158] U.S. Telecom Ass'n v. FCC, *supra* note 8, at 96–97.

[159] 47 U.S.C. § 503(b).

[160] *Id.* § 503(b)(1)(B).

ly as the basis for injunctive relief, whether applied case by case or by through a rulemaking.

VII. Legal Uncertainty over Whether 201(b) Covers Marketing Suggests the FCC Should Harmonize with the FTC.

Back in 2000, Commissioner Harold Furchtgott-Roth argued that:

> The FCC has neither the authority nor the ability to be the "marketing police" of the telecommunications industry…. The plain meaning of the term "practices" taken in the context of Section 201 does not clearly reach advertising. Indeed, if "practices" includes advertising, then it is hard to imagine what it does not include.[161]

Commissioner O'Rielly recently reiterated this view in his objection to six NALs.[162] If they are correct, that does not leave consumers unprotected; it merely shifts the authority over common carrier marketing practices from the FCC to the FTC. As the two agencies recently noted in their joint Memorandum of Understanding to govern the jurisdictional uncertainty created by the Open Internet Order's reclassification of broadband: "The agencies express their belief that the scope of the common carrier exemption in the FTC Act does not preclude the FTC from addressing non-common carrier activities engaged in by common carriers."[163] In other words, the FCC would police common carrier practices *other* than marketing claims, which would be left to the FTC. This Memorandum of Understanding is not unusual: In situations where multiple agencies have reasonable bases for asserting authority to regulate the same subject matter, they often cooperate to develop enforcement practices and provide regulated entities guidance as to the matters for which each agency is responsible.[164]

---

[161] Business Discount Plan, Inc. Apparent Liability for Forfeiture, *Order of Forfeiture*, 15 FCC Rcd 14461, 14475 (2000), *available at* https://goo.gl/20hFGX (Furchtgott-Roth, Comm'r, dissenting).

[162] O'Rielly dissent, *supra* note 52.

[163] FCC-FTC Consumer Protection Memorandum of Understanding, at 2 (Nov. 16, 2015), *available at* https://goo.gl/f7JCzM.

[164] *See* Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131, 1155–1181 (2012) (chronicling tools of agency coordination); *see also, e.g.*, Memorandum of Understanding Between The Federal Trade Commission and The Food and Drug Administration (*available at* http://goo.gl/pJYtTA) (clarifying that FTC has primary authority over advertising for foods, drugs, devices, and cosmetics, while the FDA has primary authority over branding and labeling of such materials).

Commissioners Furchtgott-Roth and O'Rielly make sound arguments, citing the FCC's past use of Section 201(b). Of course, the FCC could attempt to dismiss those arguments, arguing that the scope of the term "practices" in Section 201(b) is ambiguous, claiming *Chevron* deference, and citing the Supreme Court's recent decision in *City of Arlington v. FCC*. Justice Scalia, writing for the majority, put it thusly:

> judges should not waste their time in the mental acrobatics needed to decide whether an agency's interpretation of a statutory provision is "jurisdictional" or "nonjurisdictional." Once those labels are sheared away, it becomes clear that the question in every case is, simply, whether the statutory text forecloses the agency's assertion of authority, or not. The federal judge as haruspex, sifting the entrails of vast statutory schemes to divine whether a particular agency interpretation qualifies as "jurisdictional," is not engaged in reasoned decisionmaking.[165]

Thus, both the FCC and FTC have reasonable claim to govern the marketing of ISPs, so rather than having either or both agencies try to wrangle for jurisdictional supremacy, the FCC should simply take the initiative to harmonize its approach with that of the FTC, as that will provide the utmost certainty and consistency for regulated entities in this space.

VIII. Conclusion

This process would be unnecessary if the FCC had heeded our advice to refrain from reclassifying broadband Internet access services as common carriers. But now that the agency has embarked on this voyage, it has proposed privacy rules that rest on shaky legal authority, and lack the kind of evidentiary foundation and analytical rigor that ought to be required for regulating the Internet. We urge the FCC to put this rulemaking on hold while the litigation over reclassification is resolved and, in any event, to issue a further notice of proposed rulemaking before proceeding to final rules.

[165] City of Arlington, Tex. v. FCC, 133 S. Ct. 1863, 1870–71 (2013).