Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers	)	WC Docket No. 16-106
of Broadband and Other	)	
Telecommunications Services	)	

COMMENTS OF THE INTERNATIONAL CENTER FOR LAW & ECONOMICS AND SCHOLARS OF LAW & ECONOMICS

MAY 27, 2016

ICLE | 3333 NE Sandy Blvd. Suite 207 | Portland, OR 97232 | 503.770.0076
icle@laweconcenter.org @laweconcenter | www.laweconcenter.org

These Comments are submitted by the International Center for Law & Economics on behalf of itself, as well as the following scholars of law & economics (affiliations provided for identification only):

Babette E. Boliek	Associate Professor of Law, Pepperdine School of Law
Adam Candeub	Professor of Law, Michigan State University College of Law
Justin (Gus) Hurwitz	Assistant Professor of Law, Nebraska College of Law
Daniel Lyons	Associate Professor, Boston College Law School
Geoffrey A. Manne	Executive Director, International Center for Law & Economics
Paul H. Rubin	Samuel Candler Dobbs Professor of Economics, Emory University Department of Economics

I. Introduction

The Commission's NPRM would shoehorn the business models of a subset of new economy firms into a regime modelled on thirty-year-old CPNI rules designed to address fundamentally different concerns about a fundamentally different market. The Commission's hurried and poorly supported NPRM demonstrates little understanding of the data markets it proposes to regulate and the position of ISPs within that market. And, what's more, the resulting proposed rules diverge from analogous rules the Commission purports to emulate. Without mounting a convincing case for treating ISPs differently than the other data firms with which they do or could compete, the rules contemplate disparate regulatory treatment that would likely harm competition and innovation without evident corresponding benefit to consumers.

Concerns relating to online privacy have been extensively studied by regulators and others over the past two decades. By and large, regulators responded to these concerns with a combination of a general case-by-case approach alongside tailored rules derived from the relevant information involved in particular areas of privacy concern. Few, if any, regulators have adopted an "opt-in" privacy regime for non-sensitive data such as the FCC proposes. The FCC's proposed regime may have been cutting-edge in the 1980s and 1990s — but it

makes no sense in today's information economy in which firms from different segments of the economy fluidly enter each other's markets and effectively compete in a separate, cross-sector, informatics and advertising market. The proposed rules instead dig in the heels of the Commission against the irresistible tide of progress, attempting to maintain arbitrary industry firewalls between firms.

The "problem" the Commission attempts to fix with this proposed rulemaking is not one of preventing ISPs from using personal information to prevent new entrants from effectively competing with their incumbent businesses — which was, in fact, the genesis of the CPNI rules.[1] Rather, these rules are designed to keep *ISPs* from competing with edge providers like Google, Facebook, and Netflix.

But, in truth, both edge providers and ISPs actually need general rules of broad applicability. This is what the FTC and other regulators have largely done to date. Such broadly applicable rules are designed to be competitively neutral, and to offer the flexibility needed to address the various concerns that may come up in these markets while balancing legitimate economic and privacy interests and providing an adequate level of notice to those subject to regulation about their expected norms of conduct.

In short, the Commission has not made a convincing case that discrimination between ISPs and edge providers makes sense for the industry or for consumer welfare. The overwhelming body of evidence upon which other regulators have relied in addressing privacy concerns urges against a hard opt-in approach. That same evidence and analysis supports a consistent regulatory approach for all competitors, and nowhere advocates for a differential approach for ISPs when they are participating in the broader informatics and advertising markets. Absent the collection and analysis of substantial evidence — which at this point has not been articulated by the Commission or those advocating the Commission's proposed approach, and which is far beyond the scope of the present NPRM — the proposed approach is not supportable.

And all 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*.[2] Compared to blunt, prescriptive rules, such an approach reduces the likelihood

---

[1] *See, e.g.*, HAROLD FELD, ET AL., PROTECTING PRIVACY, PROMOTING COMPETITION: A FRAMEWORK FOR UPDATING THE FEDERAL COMMUNICATIONS COMMISSION PRIVACY RULES FOR THE DIGITAL WORLD 12 (Feb. 2016), *available at* https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper(1).pdf ("The Senate version of the Telecommunications Act of 1996, S.652, essentially followed the approach of the FCC in focusing primarily on restricting the use of information collected by ILECs from competitors."). *See also id.* at 16 ("Section 222(b) is clearly a pro-competition provision, which limits the ability of telecom providers to use information disclosed by other telecom providers to provide competing service.").

[2] *TerraCom, Inc. and YourTel America, Inc. Apparent Liability for Forfeiture*, File No.: EB-TCD-13- 00009175, Notice of Apparent Liability, 29 FCC Rcd 13325, 13335-40, ¶¶ 31-41 (2014) [hereinafter "*TerraCom*"].

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.

II. New wine in old bottles: Forcing modern business models into antiquated regulations

"The intersection of privacy and technology is not new."[3] Those are the very first words of this NPRM. And yet the Commission proposes a privacy regulatory regime for the ISPs that is essentially disconnected from the collective wisdom of the agencies, scholars and policy makers that have been operating in this space for decades. The overwhelming conclusion of this intense scrutiny is that there is no clear consensus about the proper way to deal with the intersection of innovative business models, online activity, and consumer privacy.[4] Other U.S. privacy regulations evidence more restraint and assess trade-offs, recognizing that the authorized collection and use of consumer information by data companies confers enormous benefits, even as it entails some risks.

The NPRM is positioned as a *gap filler* — as a way to apply the existing "federal privacy regime" to communications services that were removed from that regime by the reclassification of broadband Internet service under Title II:

> [T]he current federal privacy regime, including the important leadership of the Federal Trade Commission (FTC) and the Administration efforts to protect consumer privacy, does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks. That is a gap that must be closed, and this NPRM proposes a way to do so by securing what Congress has commanded — the ability of every telecommunications user to protect his or her privacy.[5]

One would think that such a set-up would engender proposed rules aimed at actually replicating the current "federal privacy regime." One might further expect the adoption of the

---

[3] Notice of Proposed Rulemaking, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket 16-106, at ¶ 1 (Mar. 31, 2016), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf [hereinafter "NPRM"].

[4] *See, e.g.*, PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES (2012).

[5] NPRM at ¶ 2.

standards enforced by the FTC under Sections 5(a) and (n) of the FTC Act, the importation of the FTC's Unfairness Policy Statement, and a commitment to the FTC's case-by-case approach to privacy enforcement. Instead the Commission seeks to impose a prescriptive privacy regime upon a small segment of the Internet ecosystem that is nowhere else replicated in the federal regulatory regime.

There is a world of difference between a regulatory regime based on suggested best practices, industry codes of conduct and overarching consumer protection standards in which businesses are free to experiment and compete within the general limits of "transparency, choice and data security," and a prescriptive regime that pays lip service to such standards but imposes aggressive constraints that fundamentally limit competition and choice.

In a remarkable and telling irony, the Commission claims that a rule that imposes "separate consent… is good for consumers and it is good business, as the success of opt-in provisions in other contexts demonstrates."[6] It then cites to only two examples of individual, privately adopted opt-in mechanisms by edge providers, Google and Yahoo.[7] It does not cite to regulatory regimes that impose such requirements. In one fell swoop the NPRM highlights both the wide gulf between the regulatory regime under which edge providers operate and the one it seeks to impose on ISPs — edge providers' potential and actual competitors — as well as the aberrant and anticompetitive nature of its rules that would limit precisely the sort of choice that permitted Google and Yahoo to adopt their preferred privacy policies.

Such specific and aggressive rules are unjustifiable given the technological and cultural realities of the day.

Moreover, the Commission's proposed rules would harm consumers who do not view privacy protections through the same, maximalist lens as the Commission. The net result of these rules is that, on the margin, consumers will be presented with a narrower range of pricing and product options, meaning that fewer consumers — who have a wide range of heterogeneous preferences — will be offered their preferred options. Consumer welfare will consequently decrease.

It is possible that the privacy-sensitive among us might be willing to pay for ad-free (and other non-tracking) versions of today's apps and other online services (including, potentially, broadband access), just as it is possible that they would be willing to bear the cost of finding and using ad- and cookie-blockers. But most people prefer to access apps, content, and services for free,[8] and don't care much about privacy[9] except with respect to the most sensi-

---

[6] NPRM at ¶ 12.

[7] NPRM at n. 236.

[8] *See, e.g.*, Mary Ellen Gordon, The History of App Pricing, and Why Most Apps are Free, The Flurry Blog (Jul. 18, 2013), http://blog.flurry.com/bid/99013/The-History-of-App-Pricing-And-Why-Most-Apps-Are-

tive information (e.g., healthcare data, children's educational records)[10] so long as the personal data they provide is secure and they get something of value in return.[11]

In a world without transaction costs, it wouldn't matter if we chose an opt-out or opt-in regime for online advertising: In either situation, the bargain struck between advertisers, content providers and users would result in the "right" level of sharing and use of behavioral data. But, in reality, there *are* transaction costs, and those transaction costs will directly bear both upon the choices that ISPs make in developing new services as well as the choices that consumers make in selecting those services.

a. ISPs compete in an information marketplace against firms with access to more comprehensive consumer information

i. ISPs are not telephone service providers

The Commission attempts to justify the disparity in its treatment of ISPs and edge providers by reference to the allegedly special characteristics of the former. First, it asserts that its proposed opt-in rules are "[c]onsistent with [] existing voice rules and other privacy frameworks," implying both that telephone networks demand more stringent privacy rules and that broadband networks are the same as telephone networks. Chairman Wheeler has argued that

> [t]he information collected by the phone company about your telephone usage has long been protected information. Regulations of the Federal Communications Commission (FCC) limit your phone company's ability to repurpose and

---

Free; Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks (The Facebook Case)* (ACM Workshop on Privacy in the Electronic Society 2005), *available at* http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

[9] *See, e.g.*, Alastair R. Beresford, Dorothea Kübler, Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* (SFB 649 Discussion Paper 2011-010, 2011), *available at* http://edoc.hu-berlin.de/series/sfb-649papers/2011-10/PDF/10.pdf; Jens Grossklags & Alessandro Acquisti, *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, *in* PROCEEDINGS OF SIXTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2007), *available at* http://weis2007.econinfosec.org/papers/66.pdf.

[10] Thus certain sector-specific privacy regimes do impose opt-in requirements in certain cases. *See* 45 CFR 164.508 (HIPAA); 34 CFR 99.30 (FERPA). But these are outliers, and they arise in clearly exceptional areas. The sort of data with which the FCC is concerned in this rulemaking is decidedly not of this sort.

> resell what it learns about your phone activity. The same should be true for information collected by your ISP.[12]

But ISPs are actually fundamentally different than phone networks. Indeed, the analogy between ISPs and phone networks quickly breaks down under analysis.

> The Internet isn't simply a telephone network with greater bandwidth; it's an entirely different approach to telecommunications. Hence, Internet regulations need to depart from the telephony model. The best option is to look toward non-technology-based frameworks, such as those developed in competition and consumer protection contexts.[13]

Switched telephone networks run on fixed hardware that provides a uniform, single-function, two-way voice service; broadband internet, on the other hand, is a generalized system that requires the interaction of a number of different types of technology in order to facilitate the timely delivery of packets.[14]

ISPs are forced to manage bandwidth in a way and with a degree of complexity that traditional phone providers rarely if ever had to. The amount of information that phone companies require in order to provide their service is relatively small, whereas ISPs must leverage a much larger body of data to understand both the technical and more subjective needs of their users.

The network infrastructure management that ISPs are required to perform gives them a unique ability to understand what their users want or need, and to understand how to better deliver it. This function of ISPs quickly moved beyond the narrowly constrained world of switched phone networks.

At the same time, ISPs deliver an invaluable public service by tailoring their offerings with varying price tiers — even free under some circumstances — and shepherding network resources more efficiently among its consumers. This requires data, and lots of it.

Thus Chairman Wheeler's exhortation that ISPs be treated like switched phone networks for the purposes of privacy betrays the fact that the Commission is operating with an ex-

---

[12] Tom Wheeler, *It's Your Data: Empowering Consumers to Protect Online Privacy*, HUFFINGTON POST (Mar. 10, 2016) *available at* http://www.huffingtonpost.com/tom-wheeler/its-your-data-protect-online-privacy_b_9428484.html.

[13] RICHARD BENNETT, DESIGNED FOR CHANGE: END-TO-END ARGUMENTS, INTERNET INNOVATION, AND THE NET NEUTRALITY DEBATE 38 (2009), *available at* http://www.itif.org/files/2009-designed-for-change.pdf.

[14] *See, e.g., The Internet and the Public Switched Telephone Network*, INTERNET SOCIETY, *available at* https://www.internetsociety.org/sites/default/files/The%20Internet%20and%20the%20Public%20Switched%20Telephone%20Network.pdf.

tremely limited understanding of this marketplace, particularly with regards to data and advertising.

ii. ISPs do not have uniquely comprehensive access to user data

The NPRM cites multiple times to the FTC's statement in its 2012 Privacy Report that "ISPs are… in a position to develop highly detailed and comprehensive profiles of their customers — and to do so in a manner that may be completely invisible."[15] The FCC uses this language to bolster its case that ISP collection and use of consumer data creates unique concerns, and that they should thus be regulated differently, consistent with the FTC approach:

> Providers of BIAS ("broadband providers") thus have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-commerce site simply does not. And they have control of a great deal of data that must be protected against data breaches.[16]

Importantly, however, the FTC Report tempers its concern that ISPs' have an exceptional ability to collect information, noting, with a nuance lacking in the NPRM, that:

> [A]ny privacy framework should be technologically neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.[17]

Taken as whole, the 2012 FTC Privacy Report does not establish the proposition that ISPs should be held to a higher (or even a different) standard of regulation than edge providers.

> This point was further emphasized in the FTC's December 2012 workshop, "The Big Picture: Comprehensive Online Data Collection," in which consumer and industry advocates alike expressed support for a technology-neutral approach. After conducting the workshop and considering the comments, the FTC did not alter the 2012 Principles or guidance, and it did not propose different rules for such providers…. Because the FCC is not in a position to dictate privacy rules for the entire Internet ecosystem, it should strive to harmo-

---

[15] NPRM at ¶¶ 4, 265 (quoting Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 55056 (Mar. 26, 2012), *available at* http://go.usa.gov/csYRz [hereinafter 2012 FTC Privacy Report]).

[16] NPRM at ¶ 4.

[17] 2012 FTC Privacy Report at 56.

> nize its proposed rules with the FTC approach and other U.S. privacy laws, and carefully consider the consequences of failing to do so.[18]

Elsewhere the NPRM claims that "broadband providers have direct access to potentially all customer information…" and supports its claim solely by a citation to a non-analytical advocacy letter signed by "59 Public Interest and Consumer Groups."[19] When non-evidence "evidence" is offered as the only basis for such a claim, there is reason to suspect that the actual evidence to support the contention simply doesn't exist.

Without citation or evidence, the NPRM makes a number of claims about ISPs' allegedly exceptional ability to view consumers' data:

- "[A] consumer, once signed up for a broadband service, simply cannot avoid that network in the same manner as a consumer can instantaneously (and without penalty) switch search engines (including to ones that provide extra privacy protections), surf among competing websites, and select among diverse applications."
- "[A]bsent use of encryption, the broadband network has the technical capacity to monitor traffic transmitted between the consumer and each destination, including its content. Although the ability to monitor such traffic is not limitless, it is ubiquitous."
- "Even when traffic is encrypted, the provider has access to, for example, what websites a customer has visited, how long and during what hours of the day the customer visited various websites, the customer's location, and what mobile device the customer used to access those websites."[20]

In fact, non-ISP information collection practices are frequently far more robust than those of ISPs. In Appendix A to this Comment we detail the data collection practices of the most common types of non-ISP companies. In some cases (e.g., browsers, advertising networks and operating systems) the breadth of data collected from a wide range of sources is substantial, and substantially greater than for ISPs. As Peter Swire notes,

> ISP access to user data is not comprehensive — technological developments place substantial limits on ISPs' visibility. Second, ISP access to user data is not unique — other companies often have access to more information and a wider range of user information than ISPs.[21]

---

[18] Letter of Jon Leibowitz to the FCC, RE: Protecting the Privacy of Broadband and Other Telecommunications Services, WC Docket No. 16-106, at 7 (May 23, 2016), *available at* http://apps.fcc.gov/ecfs/document/view?id=60002014604 [hereinafter "Leibowitz Letter"].

[19] NPRM at n. 237.

[20] NPRM at ¶ 4.

[21] Peter Swire, Justin Hemmings & Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, THE INSTITUTE FOR INFORMATION SECURITY & PRIVACY AT GEORGIA TECH at 7 (Feb. 29, 2016) [hereinafter "*Online Privacy And ISPs*"].

Compared to their edge-provider and other analogues, ISPs do not have particularly broad insight into consumer data that is not given to them in the course of subscribing:

> In most cases, ISPs have relatively accurate information about a subscriber's name and billing address, and may have their credit card information and phone number. [But beyond that,]… users today often connect to the Internet with multiple devices and from multiple locations, and at far higher speeds. This means that any single ISP views a diminishing portion of a user's Internet activity, and that the portion they do not carry represents an enormous and growing volume of data and transactions. Second, encryption is becoming pervasive…. With encrypted content, ISPs cannot see detailed URLs and content even if they try. Third, multiple changes, including widespread use of Virtual Private Networks ("VPNs") and third-party proxy services, are further limiting ISP visibility.[22]

b. Opting-in to consumer harm: The unsupported benefits and disregarded harms of the Commission's proposed opt-in rules

Apart from its failures to justify treating ISPs differently than other competitors, and apart from its failure to justify more stringent treatment for ISPs in general, the NPRM also fails to justify the specific rules it prescribes. Of most significance is the imposition of an opt-in requirement for the sharing of non-sensitive data.

The Commission asserts that this rule is needed because,

> in an era in which broadband providers are or may be affiliated with content providers, social networks, or companies that serve online ads and forms of social media, **opt-in approval is needed to protect the reasonable expectations of consumers, who may not understand that their broadband provider can sell or otherwise share their information with unrelated companies for diverse purposes (such as targeted advertising), or can repurpose customer information for such purposes**….[23]

> [C]ustomers desire and expect the opportunity to affirmatively choose how their information is used for purposes other than marketing communications-related services by their provider and its affiliates.[24]

---

[22] *Id.* at 23.

[23] NPRM at ¶ 18 (emphasis added).

[24] NPRM at ¶ 127.

The mere fact, however, that a consumer's information may be used in ways that the user doesn't expect or understand does not mean that such use is harmful to consumers individually or in the aggregate. Whether such uses are desirable, or on net are beneficial or harmful to consumers, is an empirical question — one that has been extensively researched:

> "Opt-in" is frequently portrayed as giving consumers greater privacy protection than "opt-out." In fact, the opposite is true. "**Opt-in" provides no greater privacy protection than "opt-out" but imposes significantly higher costs with dramatically different legal and economic implications**.[25]
>
> **[T]he opt-out regime produces better welfare results than the anonymity regime, which in its turn is better than the opt-in regime.** Therefore, from a social welfare point of view, it matters whether opt out or opt in is adopted as the privacy standard.[26]

And, of course, an opt-in regime is indeed more expensive than an opt-out regime.[27] In fact, Fred Cate and Michael Staten offer a particularly apt example drawn from telecommunications:

> [C]onsider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system. In obtaining permission to utilize information about its customer's calling patterns… the company found that **an "opt-in" system was significantly more expensive to administer, costing almost $30 per customer contacted**. To gain permission to use such information for marketing, U.S. West determined that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, **many U.S. West customers received more calls than in an "opt-out" system, and one-third of their customers were denied opportunities to receive information about valuable new products and services.**[28]

---

[25] *See* Fred H. Cate & Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In"* 1 (2003), *available at* http://home.uchicago.edu/~mferzige/fallacyofoptin.pdf.

[26] Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis Of Privacy Policies* 5 (CESifo working paper, No. 1831, 2006), *available at* https://www.econstor.eu/bitstream/10419/25876/1/521168813.PDF (emphasis added).

[27] *See* Cate & Staten, *supra* note 25; Nicklas Lundblad and Betsy Masiello, *Opt-in Dystopias*, SCRIPTED (2010), *available at* http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

[28] Cate & Staten, *supra* note 25, at 5 (emphasis added).

The core of the problem with an opt-in regime is that it staunches the flow of data, imposing both direct and indirect costs on the economy and on consumers.[29] This reduces the value of certain products and services not only to the consumer who does not opt-in, but to the broader network as a whole.

At the same time, empirical research shows that opt-in privacy rules reduce competition by deterring new entry. The seemingly marginal costs imposed on consumers by requiring opt-in can have a significant cumulative effect on competition:

> [P]rivacy regulation imposes transaction costs whose effects… will fall disproportionately on smaller firms. **Consequently, rather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive**…. Under regulation, the extra costs required to obtain consent mean that in some cases where entry had been profitable without regulation, [some firms] will choose not to enter.[30]

On net opt-in regimes may tend to favor the status quo, and to maintain or grow the position of a few dominant firms. Opt-in imposes additional costs on consumers and hurts competition — and it may not offer any additional protections over opt-out. In the absence of any meaningful evidence or rigorous economic analysis to the contrary, the Commission should eschew imposing such a potentially harmful regime on broadband and data markets.

III. Damaging markets, distorting competition, and defeating consumer preferences

a. Harms to competition and business model distortion

Despite the Commission's recognition that "edge providers, who may have access to some similar customer PI, are not subject to the same regulatory framework, and that this regula-

---

[29] *Id.* at 5:

> There is a stark difference between "opt-in" and "opt-out" in terms of cost…. [T]he "opt-out" system sets the default rule to "free information flow" and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an "opt-in" system presumes that consumers **do not want** the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them…. cost. … Consequently, an "opt-in" system for giving consumers control over information usage **is always more expensive than an "opt-out" system**. (emphasis in original).

[30] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT STRATEGY 47, 48-49 (2015) (emphasis added).

tory disparity could have competitive ripple effects,"[31] it nonetheless believes that competition will not be distorted. The NPRM lists several bases for this conclusion, including that the FTC will continue to police edge providers for "unfair" conduct, that "industry has developed guidelines recommending obtaining express consent before sharing some sensitive information," and that, in some fashion, edge providers have access to only a limited amount of information.[32]

This is a thin reed on which to hang its defense of disparate treatment. All of the stated reasons are either aspirational or simply reassert that the standards applied to ISPs and edge providers are different.

But the problems created by this differential treatment aren't simply a matter of "fairness." Rather, the differing privacy rules can have significant consequences for the organization of businesses and the structure of markets. To the extent that more aggressive rules impose greater costs on some entities compared to others, or distort markets by deterring entry, the effect will be an overall reduction in competition and efficiency, resulting in harm to consumers.

Further, to the extent that the proposed rules would apply only to ISPs, they create a regulatory asymmetry that will likely distort competition and, ultimately, harm innovation and consumer welfare.

And the NPRM will have negative unintended consequences that may "require" further agency intervention in the future in order to resolve. The Commissioners claim that they

> are mindful that in adopting a framework for customer approval for use by and disclosure to affiliates of customer PI, we do not want to inadvertently encourage corporate restructuring or gamesmanship driven by an interest in enabling use or sharing of customer PI subject to less stringent customer approval requirements. We believe that we can discourage such gamesmanship by treating use by an affiliate as subject to the same limits as use by a BIAS provider.[33]

In other words, to make the rules workable, they must extend further than just ISPs. As companies seek to innovate around rules that quickly become outdated, the Commission

---

[31] NPRM at ¶ 132.

[32] Apparently the information that edge providers have access to is limited only to the extent that the consumers engage with the edge provider's services, whereas the Commission feels that ISPs have access to "potentially all customer information." NPRM at ¶ 132. The Commission seems to be of this opinion despite research that shows that many factors confound a BIAS provider's ability to access consumer information — including increases in encryption. *See generally Online Privacy and ISPs*, *supra*.

[33] NPRM at ¶ 124.

will be left in a position to either acquiesce in its relative inability to impose its rules or intervene in an expanding array of situations beyond its mandate and further and further out toward the edge.[34]

Likely, however, and regardless of whether the Commission chooses to play a game of "business model whack-a-mole," ISPs will be required to warp their business methods in order to accommodate both consumer expectations and market and technological realities while navigating the rules. And, of course, there is a serious risk that business model changes adopted for reasons having nothing to do with evading the FCC's rules will be perceived by the Commission as "gamesmanship," leading it to over-enforce its rules in order to "protect" its jurisdiction.

b. The edge will inevitably be affected

Even if the FCC can restrain itself for the time being from extending its privacy rules to the edge, the rules will still affect far more than just ISPs. Although initially edge providers will possibly benefit from the new regulations on ISPs by making it more difficult for ISPs to compete in markets for data and online advertising, in the long run both edge providers and consumers will suffer under the rules alongside the ISPs.

This is because the NPRM invariably will have effects much larger than the FCC seems to appreciate. While Chairman Wheeler insists that "this [proposed rule] is not regulating what we often refer to as the edge"[35] and that "this is about ISPs and only ISPs",[36] the rules will inevitably affect the Internet ecosystem well beyond ISPs. Edge providers need not be the direct object of regulation to be affected by it. And consumers, who may make privacy decisions based on these rules, will be unable to make meaningful decisions about edge provider privacy practices.

Moreover, the Commission's claim to regulate only ISPs fails along a second dimension. This NPRM is clearly not solely about "ISPs and only ISPs" insofar as the rules would put a regulatory thumb on the scale well in favor of edge providers. As we discuss, *infra*, competition among firms based upon data is not limited to firms within firewalled industries — competition for advertising and consumer attention more broadly occurs across industries and firms. For example, although the point is often misunderstood, Google competes directly with Facebook for search-based revenues, even though Facebook is a "social media site" and Google is a "search engine." No less do ISPs compete with edge providers for the value

---

[34] *See generally* LUDWIG VON MISES, A CRITIQUE OF INTERVENTIONISM (1977).

[35] NPRM at ¶ 135.

[36] John Egerton, *Senators Vet FCC Broadband CPNI Proposal*, MULTICHANNEL NEWS (May 11, 2016) *available at* http://www.multichannel.com/news/congress/senators-vet-fcc-broadband-cpni-proposal/404841.

in their ad networks and user attention. Even though an ISP provides broadband access in its primary role — just as Google provides search results in its primary role — ISPs can extend their value proposition by being able to tailor services to consumers through data use and deliver valuable consumer attention to advertisers — exactly as Google does with its advertising networks.

And while the FCC disclaims any desire to extend its privacy rules to the edge, the legal authority and reasoning they use to justify these rules almost compels this result. The FCC asserts that Section 706 of the Communications Act could be a basis of authority for its privacy rules.[37] If consumers complain to the FCC about what are actually edge services allegedly violating consumer privacy (as self-appointed Consumer Watchdog did[38]), the FCC could easily use Section 706 as a justification for extending regulations to the edge that are, in the Commission's view, necessary in order to promote the "virtuous cycle."[39]

The logic for this extension is implicit in the terms of the rules. According to the NPRM, "since they have the potential to increase customer confidence in [edge] providers' practices, thereby boosting confidence in and therefore use of [edge] services,"[40] and "new uses of the network...lead to increased end-user demand for broadband, which drives network improvements,"[41] presumably extending privacy rules to the edge would encourage "deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[42]

c. International harms

The NPRM also has the potential to create international confusion among regulators. The United States government has long taken the position that the FTC's model of privacy regu-

---

[37] NPRM at ¶ 309.

[38] Dismissal of Petition for Rulemaking, *Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor 'Do Not Track' Requests*, FCC DA-1266 (Nov. 6, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1266A1_Rcd.pdf.

[39] For instance, in its Open Internet Order, the Commission observed that "consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth." In the Matter of Protecting and Promoting the Open Internet," *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) [hereinafter "OIO"]. While this conversation was couched in a discussion of Section 222, the very same logic can be employed to drive edge provider regulations under Section 706.

[40] *Cf.* NPRM at ¶ 309.

[41] OIO at ¶ 77.

[42] NPRM at ¶ 309.

lation and enforcement provided consumers with robust protection.[43] The FCC's dramatically different approach suggests the FTC's model was not good enough and may diminish the ability of the United States to advocate on behalf of its interests abroad. Particularly in light of the fact that various negotiations and court cases within the EU are ongoing around the issue of consumer privacy, [44] the proposed rules threaten to upset the balance of expectations for each side of the ongoing negotiations.

d. Yet more harm for consumers

In addition to the problems discussed above, the NPRM will harm consumers in three distinct ways. First, it will likely drive services that consumers value out of the market. Second, it can create consumer confusion regarding privacy owing to the disparate treatment of edge providers and ISPs. Third, it will likely distort revenue models in a way that is likely to drive prices for broadband access higher.

i. Consumers value personalized services

While the FCC nods to the fact that consumers value personalized services powered by data, the rules severely limit the ability of ISPs to provide these services. As we have learned in the mobile app market, for instance, a significant number of consumers have a strong preference for nominally free (zero price) apps that make use of their personal information to serve up relevant ads over paid apps.[45] Further, research suggests that consumers may be broadly indifferent to the privacy implications of their online behavior.[46] And, of course, many consumers might simply prefer a higher-quality service that provides superior insights

---

[43] *See* Jedidiah Bracy, *How Julie Brill is Cultivating a Defense of the U.S. Privacy Framework*, PRIVACY PERSPECTIVES (Feb. 24, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/630801/150224juliebrillcultivatingprivacy.pdf.

[44] *EU-U.S. Privacy Shield: gray period for businesses*, Ecommerce Europe (Feb. 18. 2016), *available at* http://www.ecommerce-europe.eu/news/2016/eu-u.s.-privacy-shield-gray-period-for-businesses; Jedidiah Bracy, *Model clauses in jeopardy with Irish DPA referral to CJEU*, IAPP (May 25, 2016), *available at* https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/.

[45] Greg Sterling, *Survey: 58 Percent Prefer Ad-Based Apps To Paid, Freemium Models*, MARKETING LAND (Oct. 26, 2014), available at http://marketingland.com/survey-proclaims-consumer-preference-ad-supported-apps-daa-readies-mobile-appchoices-105463.

[46] *See generally* Ralph Gross and Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks (The Facebook case)* (ACM Workshop on Privacy in the Electronic Society 2005), *available at* http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

through better engineered algorithms[47]— something that would undoubtedly be facilitated by ISPs' ability to gain insights from consumer data.

Although some segment of consumers will be better off under the rules — by, for instance obviating the need for those consumers to search for services that offer more privacy — many more consumers will be made much worse off by removing the options from the market that allow them to forego some level of privacy protection in exchange for more affordably priced services.

And, at root, severely limiting ISPs from being able to use customer data is based on a fundamental misunderstanding of the value of such data. In itself, the value of a particular piece of information about a consumer is intrinsically zero (or nearly so) — knowing someone's birthday is an empty bit of trivia to a firm, for instance. However, knowing someone's birthday becomes a valuable piece of information when a firm can then offer special discounts or other gifts as part of outreach to that consumer on their birthday. Thus the core of the value is not actually the information itself, but is instead the value the consumer attaches to receiving the more personal connection with a firm that enables highly tailored goods and services.

In order to create better fit between raw data and valuable services, companies, especially new entrants like ISPs in data markets, need to be able to experiment. Unfortunately, the proposed rules deter experimentation and expansion into new markets. For instance, according to the rules, ISPs must "[e]xplain that a denial of approval to use, disclose, or permit access to customer PI for purposes other than providing BIAS will not affect the provision of any services to which the customer subscribes."[48] However, what if the use of data is used to finance the provision of certain services? If direct advertising is being sold based on targeted information, and that targeted information is derived from opt-in customers, then if a customer opts-out the BIAS provider *must* terminate access to that service. Therefore, the rules directly foreclose a number of potential business models with this one apparently simple paragraph.

Further, the Commission "propose[s] to adopt rules permitting ISPs to use customer PI for the purpose of marketing additional BIAS offerings in the same category of service … to the customer, when the customer already subscribes to that category of service from the same

---

[47] *See* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013), *available at* http://www.georgemasonlawreview.org/wp-content/uploads/2014/03/Cooper_Website.pdf.

[48] NPRM at ¶ 106.

provider[.]"[49] Otherwise, the ISPs would have to "obtain customer opt-in approval for the use and sharing of all customer PI."[50]

Typically, this sort of regime is reserved for the most sensitive of data; treating it as an industry-wide default rule for a fast-paced, evolving marketplace diverges from the existing "federal privacy regime" and will do far more harm than good. This approach to customer information essentially destroys the ability of providers to market potential add-on or complementary services which, in combination, may provide efficiencies that justify lowering costs to the consumer. For example, a provider would be prevented from marketing new telephone service to existing broadband customers or an innovative package that would allot a data pool across mobile and fixed broadband. Firms in the broadband market need to be able to experiment with new financing models, product innovations, and so forth, in just the same way that edge providers do. But these rules will deter any such innovation. The aim of any regulation of business practices that trade information for nominally free services should be to strike the proper balance between consumer desires and service provider capabilities. But the Commission's proposed rules fail to perform even a rudimentary cost-benefit analysis—it "propose[s] to prohibit the offering of broadband services contingent on the waiver of privacy rights by consumers," thus belying a fundamental misunderstanding that in addition to the costs associated with "paying" with information, consumers undoubtedly benefit as well.

At a minimum, the Commission should conduct a probing economic analysis of the relative costs and benefits to all consumers before aggressively launching on a course that will undoubtedly harm consumers.

ii. Consumer confusion

Consumers are unlikely to know that different regulatory regimes apply to ISPs and edge providers. Privacy sensitive individuals may then blame ISPs for things like targeted advertising due to edge services collecting information on them. These individuals may then bring consumer complaints to the FCC against ISPs. Even if the FCC sincerely does not wish to extend rules to the edge, consumer complaints and confusion may artificially generate the need for the Commission to so extend the rules.

Strong privacy rules can have unintended and harmful effects on consumers, particularly the least-well-off. Aside from the direct price effects from limiting the substitution of advertising- and data-based revenue models for direct payments, compliance costs and indirect limits on innovation and competition can raise prices.

---

[49] *Id.* at ¶ 114.

[50] *Id.* at ¶ 126.

Prescriptive privacy rules constrain consumer choice by precluding some consumers who would otherwise do so from transacting on the basis of their own privacy preferences. But such rules also harm consumers by imposing excessive compliance costs on all businesses and by limiting the creation and marketing of new products and services. Thus, rules like the ones proposed in the NPRM that purport to promote the "core principle" of "choice," may do precisely the opposite.

At the same time restrictive privacy rules impose direct and indirect costs that fall disproportionately on the poor:

> The benefits and burdens of privacy protection are not distributed equally over rich and poor. Privacy protection is a superior (or luxury) good, which implies that the demand for it is not only a negative function of price but also a positive function of income and wealth. The rich want more privacy protection than the poor. Consequently, privacy law has a regressive income effect and hurts the poor who are required to cross-subsidize the needs of a rich privacy elite. The poor suffer disproportionately also where they already have less choice and pay higher prices than the rich. Take, for instance, consumer credit and lending. Due to privacy law's adverse effects on the free circulation of consumer credit information, loans or credit may no longer be available to the poor or only at substantially higher interest rates; the rich, on the other hand, may not be significantly affected by the restricted flow of their credit data. Privacy protection thus indirectly causes economic and social exclusion. Similarly, a move from opt-out to opt-in in the catalog apparel sector would increase prices by up to 11% and those increases would disproportionally affect rural customers and those in less affluent city neighbourhoods. Unfortunately, these effects are not recognized, denied or at best downplayed by the various participants in the privacy debate.[51]

Similarly,

> [W]e can expect that opt-in policies may have as an unintended consequence the effect of reinforcing exclusionary effects on less technology-literate groups. A user with less technology experience when asked to evaluate a service will naturally and unavoidably face a higher cost in making that evaluation than a more technologically knowledgeable user.[52]

---

[51] Lucas Bergkamp, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy, 18 Computer Law & Security Report 31, 38 (2002).

[52] Nicklas Lundblad and Betsy Masiello, *Opt-in Dystopias*, SCRIPTED, § 5.1 (2010), *available at* http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

iii. Higher prices for broadband

ISPs are multi-sided platforms that connect their subscribers with edge providers. While ISPs have primarily relied upon a subscription revenue model, they could (absent prohibitive regulation) subsidize or replace subscription fees with edge-provider access charges, advertising revenue, or the sale of data. Platforms like Google and Facebook often use the data collected as part of their services on one side of the platform to power the advertising network on the other. ISPs could do something very similar, using data collected from its subscribers for targeted advertising — and a corresponding reduction in subscription prices or increase in investment expenditures.

Of course, the Open Internet Order effectively prohibits ISPs from charging edge providers. And this NPRM would significantly curtail the ability of ISPs to use targeted advertising as a source of revenue. By systematically removing alternative sources of revenue for ISPs — particularly in an economy that is increasingly accustomed to such revenue arrangements — the FCC's regulations will place upward pressure on consumer Internet access prices.

While some consumers may be willing to trade off higher prices for stronger privacy regulations, those consumers who might prefer the option of less privacy and lower prices will be forced to effectively subsidize the most privacy sensitive consumers. The FCC's current proposal that would ban the conditioning of Internet access on data collection, and its contemplated proposal to extend the ban even to *discounts* for data collection,[53] are misguided. Far from increasing consumer choice, they foreclose it, saddling users with higher prices and forcing some consumers to subsidize others.

---

[53] *See* NPRM at ¶¶ 258-63. As FTC Commissioner Maureen Ohlhausen notes,

> The NPRM mischaracterizes the FTC's findings about what the FCC labels "financial inducement practices" but which most people know as "discounts." The NPRM states, "the FTC and others have argued that these business models unfairly disadvantage low income or other vulnerable populations…." But the FTC did not argue this. The portion of the FTC Big Data Report cited by the NPRM merely summarizes the concerns of some workshop participants — not FTC staff — about big data uses generally. Even on that point, the FTC report observed, "big data can create opportunities for low-income and underserved communities," and cites a broad range of existing examples.

Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, at 3, WC Docket No. 16-106 (May 27, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/951923/160527fccohlhausenstmt.pdf.

IV. A better path forward

a. Regulatory parity

The future is data and its efficient use in service to overall consumer welfare. The rules explicitly contemplate hamstringing ISPs, even where edge providers will be given much looser reins. Though it is doubtful the Commission intends these rules as a harm to consumers, the lack of regulatory parity between ISPs and edge providers virtually assures that competitors will be kept out of the data and advertising markets. Thus, the rules will distort competition, and act as a barrier to competition.

Absent clear evidence — through careful economic analysis — that ISPs deserve differential regulatory treatment, they should not be subject to a different standard of conduct, particularly when such a differential standard will harm the broader market.

Moreover, the Commission seeks to impose requirements on ISPs that could lead to protracted litigation— even when the challenged conduct is not the ISPs' own. The NPRM states that ISPs would be permitted to use aggregate customer PI, so long as (among other requirements), it "contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and ... exercises reasonable monitoring to ensure that those contracts are not violated." Placing a requirement upon a BIAS provider that it police its partners for compliance with the Commission's rules would be an onerous requirement. This is particularly true given the fact that, as any lawyer will tell you, "reasonable monitoring" is a highly subjective term. Therefore, in addition to being forced out of the broader data and advertising market, ISPs will be saddled with ongoing uncertainty over even the modest uses for data which the NPRM would permit.

b. The FCC should adopt an error cost approach to privacy

In the face of a difficult cost-benefit calculus that is highly dependent on evolving technology and shifting consumer preferences — and one which, so far, the Commission has not indicated it intends to perform — a case-by-case approach that undertakes a careful analysis of each alleged privacy violation makes tremendous sense. The basic error-cost formula counsels against ex ante regulation of conduct unless such conduct "always or almost always"[54] tends to harm consumers. For the difficult cases that make up the bulk of litigated and adjudicated actions, ex ante prohibitions make little sense.

The FTC's approach to privacy regulation recognizes the substantial consumer benefits that can result from personalization and data-empowered services and (ideally) leads to en-

[54] Leegin Creative Leather Prods. v. PSKS, Inc., 127 S. Ct. 2705, 2713 (2007).

forcement only when conduct is truly harmful in light of the circumstances of a given case. The approach set forth in the FCC's proposed rules, however, is much different. Outright banning of conduct that could — and oftentimes manifestly does — offer net consumer benefit is an abdication of the Commission's obligation to act in the public interest.

Chairman Wheeler claims to admire the FTC's model.[55] The FCC even defends its approach as consistent with the FTC's best practices,[56] FTC guidance,[57] and the 2012 FTC Privacy Report.[58] But in reality the Commission and the Chairman are engaged in an unfair and deceptive effort to mislabel its approach in these rules as consistent with FTC practice.

As former FTC Chairman Jon Leibowitz (who was Chairman when the 2012 FTC Privacy Report was written) explains, the FCC's approach diverges considerably from the FTC's, especially with respect to online advertising data.[59]

For much of the Internet, online advertising data is its lifeblood. The FTC recognizes the value of data for online services and has designed its rules accordingly (i.e., opt-out consent). But for a large swath of data the FCC proposes a different approach, requiring *opt-in* consent. As former Chairman Leibowitz notes:

> Rather than narrowly tailoring a requirement for opt-in consent to truly "sensitive data," the proposed rules would impose a broad opt-in requirement upon broadband providers for the use of a wide swath of consumer data for an extensive range of practices — including practices for which the FTC requires no choice at all because implied consent is presumed. In doing so, the NPRM completely ignores the critical context of the interaction between the consum-

---

[55] Margaret Harding McGill, *FCC, FTC Chiefs Zero In On Data Security, Privacy*, LAW 360 (Jan. 6, 2016), *available at* http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy ("What the FTC has done in that regard is to build a terrific model and so I think one of our challenges is to make sure we're consistent with the kind of thoughtful, rational approach that the FTC has taken.").

[56] NPRM at ¶¶ 154, 172, and 175.

[57] *Id.* at ¶¶ 156, 157, 160, and 195.

[58] *Id.* at ¶¶ 162, 217, 220, 258, and 265.

[59] *See also* Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (May 27, 2016), at 8, *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf (noting dourly that the NPRM "would impose a number of specific requirements on the provision of BIAS services that would not generally apply to other services [such as those subject to FTC regulation] that collect and use significant amounts of consumer data. This outcome is not optimal."), *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf..").

> er and the service provider, which would make consumers the losers in this policy choice.[60]

Following the FTC, the FCC does seek to create an exemption from notice and consent for de-identified data. But even though the FCC claims its proposal is "grounded in FTC guidance,"[61] the FCC's approach to aggregated customer information actually goes much further, adopting a specific requirement that data be de-identified. Again, as former Chairman Leibowitz notes:

> The FTC framework does not govern the notice, use, disclosure, security, or notification of breach of anonymized or de-identified individual data, as long as such data cannot be reasonably linked to a particular consumer, computer, or device. The FTC excluded de-identified data because it does not present a risk to consumer privacy or security. The FCC's proposal appears to confuse the FTC's guidance on the "reasonable linkability" standard and the appropriate steps companies can take to minimize such linkability with a standard for aggregation, which is but one way to de-identify data.[62]

As we discuss above, this and other "confusions" by the FCC suggest that it simply does not understand the technology and business uses of data in the broader informatics markets that it proposes to regulate.

In brief, much online advertising is based on de-identified data. But not all of the de-identified data used by online advertisers is *aggregated* customer information, as the FCC defines it. The FTC's 2012 Privacy Report gives companies much greater flexibility in determining how to de-identify data, and defines such data much more broadly than does the FCC.

Rather than asserting — inaccurately — that it is following the FTC's approach, the FCC should actually do so. And the FCC's *TerraCom* enforcement action suggests that the Commission is *capable* of doing so.

c. The FCC should use TerraCom as a model of case-by-case enforcement

In examining the FTC's approach as a model for the proposed rules, the Commission intends to take the worst of the FTC's practice while ignoring its own fairly positive work in this area.

---

[60] Leibowitz Letter at 8.

[61] NPRM at ¶ 156.

[62] Leibowitz Letter at 6.

For instance, the Commission contemplates adopting an "unfairness" standard similar to the UDAP standard embodied in Section 5 of the FTC Act:

> Our proposal is also consistent with the approach that the FTC has taken in providing guidance on best practices for all companies under its jurisdiction, and in using the "unfairness" prong of Section 5 of the FTC Act in its enforcement work. The FTC has taken enforcement action in cases where companies have failed to take "reasonable and appropriate" steps to protect consumer data, including several dozen cases against businesses that failed to protect consumers' personal information.[63]

The Commission should take care with this approach, however.

First, the FTC's unfairness standard is not "reasonable and appropriate." Rather, the statute requires that the Commission undertake unfairness enforcement actions only when injury is substantial, unavoidable by consumers, and not outweighed by countervailing benefits.[64] The FTC has a welter of enforcement decisions, rules, industry guides, institutional memory, established practices and procedures, and its Unfairness Policy Statement to guide its enforcement decisions and — one hopes — to provide a sort of internal algorithm to convert "reasonable and appropriate" into the requisite statutory standard. The FCC has essentially none of these.

But at the same time, the FTC is arguably playing fast and loose with the statute in applying its "reasonableness" standard often ignoring (or, at the very least, not disclosing) whether and how it is adhering to the statutory requirement in Section 5(n) that it balance alleged harms against countervailing benefits. While the FTC's *model* is worthy of emulation, in execution its consumer protection enforcement practice demonstrates a number of problematic elements.[65]

Second, the Commission has already demonstrated an ability to take an FTC-like approach to privacy with its *TerraCom* decision. And that approach, broadly speaking, actually represents an *improvement* over the FTC's own process. The FTC is often criticized for its "common law of privacy" — not because it has developed one, but because it claims to have done so without offering substantive guidance in the form of opinions, closing letters or other binding legal documents.[66] The *TerraCom*, decision, by contrast, actually demonstrates the

---

[63] NPRM at ¶ 172.

[64] *See* 15 U.S.C. §45(a); 15 U.S.C. §45(n).

[65] *See generally* BERIN SZÓKA & GEOFFREY A. MANNE, THE FEDERAL TRADE COMMISSION: RESTORING CONGRESSIONAL OVERSIGHT OF THE SECOND NATIONAL LEGISLATURE — AN ANALYSIS OF PROPOSED LEGISLATION (2016), available at http://ftcreform.org/szoka___manne_-_ftc_reform_report_2.0_-_may_2016.pdf.

[66] *See id.*

sort of legal analysis that is crucial for the establishment of a common law, and the Commission should continue this case-by-case approach. [67]

In the *TerraCom* Notice of Apparent Liability, the Commission walked through a detailed analysis of both the statutory basis for its ruling, as well as an application of its authority and the relevant statutes to the particular facts at hand.[68] The Commission detailed this analysis under two separate statutory sections of the Communications Act. In its Section 222(a) analysis, for instance, the Commission devoted five pages to analyzing how to define and apply "proprietary information,"[69] "customers,"[70] and the manner in which the defendants allegedly breached their obligations to consumers.[71] It performed a similarly thorough analysis under § 201(b), explaining the basis for its opinion that the defendants had engaged in both "misrepresentations" for particularly identified improper security practices, as well as "unfair and unreasonable" practices related to a failure to notify victims of a breach.[72]

In sum, regardless of whether one agrees with the substance of the Commission's analysis in *TerraCom*, the decision offers what the FTC's data security and privacy consent orders do not: the sort of analysis that future potential subjects of investigation can rely upon in guiding their own conduct.[73]

Far from adopting an FTC-like, case-by-case model for privacy regulation, the proposed rules would completely undermine the valuable work developing its own "common law" under Section 201(b) that the Commission began with *TerraCom*.

V. Conclusion

We believe that the Commission has failed to undertake meaningful (or *any*) analysis of its proposed rules and their likely unintended consequences sufficient to justify the imposition

---

[67] It is worth noting that we do not here specifically endorse the Commission's view of its authority under §§ 222 or 201, nor its exercise of authority without a rulemaking. We merely present *TerraCom* as an example of the Commission's already demonstrated ability to handle a case-by-case analysis of privacy harms, as well as its apparent willingness to produce the sort of valuable legal analysis that can guide future parties.

[68] *See generally TerraCom, supra*, note 2.

[69] *Id.* at ¶¶18-20

[70] *Id.* at ¶¶21-26

[71] *Id.* at ¶¶28-30.

[72] *Id.* at ¶¶14-17.

[73] It is worth noting that we do not here specifically endorse the Commission's view of its authority under §§ 222 or 201, nor whether it was proper for the Commission to exercise authority as it did without first proposing a rulemaking — we merely present *TerraCom* as an example of the Commission's already demonstrated ability to handle a case-by-case analysis of privacy harms, attendant with a willingness to produce the sort of legal documentation that can guide future parties.

of its aggressive, ex ante standard for privacy practices on ISPs. There are myriad problems with the proposed rules. As we discuss, these rules would likely harming the consumers they purport to protect. We urge the Commission to reject the rules proposed in this NPRM and engage in a measured, rigorous and thoughtful assessment of the best course of action to pursue in order to ensure that its regulation of broadband provider privacy practices serves the public interest.

Appendix A: Non-ISP information collection practices

CLASS OF ENTITY	INFORMATION COLLECTION PRACTICES/EXAMPLES
WEBSITES AND E-COMMERCE	• Use cookies and other techniques to track users within a website and across websites. • In addition to credit or debit card, billing address, shipping address, email address, and phone number, an e-commerce website also "necessarily see[s] the rest of the details associated with the buyer's purchase, such as which items they bought, reviews they have left, how frequently they purchase from the seller, wish list or registry items, and items they have saved in their online shopping carts for later purchase."[74] • In an October 2012 study, the UC Berkeley Web Privacy Census found a total of 6,485 cookies on the top 100 websites; the vast majority of these were from third-party domains.[75] These tools can be used to compile substantial amounts of information about users across different sites: "even if a cookie is never attached to your name or your address, a cookie could still be associated with your behavior over time."[76]
SEARCH ENGINES	• Use automated software applications that gather information that is used to create a searchable index of the web, which in turn allows the search engine to see both the URLs and content a user selects. • The intensive use of search engines enables search engine providers to collect highly specific and personalized data.[77] • "Google processes over 40,000 search queries every second on average, which equates to over 3.5 billion searches per day and 1.2 trillion searches per year worldwide."[78]

[74] *Online Privacy and ISPs* at 97.

[75] October 2012 Web Privacy Census (Version 2.0), https://www.law.berkeley.edu/centers/bclt/research/privacy-at-bclt/web-privacy-census/october-2012-web-privacy-census/ (last visited May 21, 2016).

[76] Prof. Dan Wallach, *FTC Comprehensive Online Data Collection Workshop Transcript*, at 31 (Dec. 6, 2012).

[77] *Online Privacy and ISPs* at 51.

[78] *Id.* at 51 n.7.

WEBMAIL AND MESSAGING	• Scan email content as well as metadata, such as email addresses, time, date, and file size. • Webmail providers are not limited to scanning emails within the same webmail service, rather they can scan both incoming and outgoing emails, including emails coming from different email providers. In addition, many webmail providers are able to read emails even when they have been abandoned and are never sent, such as draft emails.[79]
BROWSERS, INTERNET VIDEO	• Track users' information and web activity through telemetry, cookies, integrating search with other functionality, and other techniques. • Even for HTTPS traffic (i.e., encrypted traffic), a web browser still has technical access to both the full URLs a user visits and the specific content of those URLs.[80] • Because internet video may be consumed through direct website browsing or through video applications viewed on a host of different devices, online video content can pass through the products and/or services of numerous software providers, hardware providers, operating system developers, and online services. These entities all have differing levels of visibility into a user's video content choices.
ADVERTISING NETWORKS	• Track users' information and web activity across ISPs, websites, and devices using multiple techniques, including cookies, to deliver targeted ads. • Use web beacons designed to blend into the background of a web page that can track site traffic, unique visitor counts, advertising efficacy, as well as personalize websites. Statistical identifiers that rely on information about a particular browser or device may also be used.[81] • Online advertising entities are "often able to use their access to URLs to then find the content that corresponds to that URL — knowing the detailed URL allows the entity to, in effect, click on the link and see the content. Entities that do this can then often associate that URL and content with other contexts and devices, giving these entities even higher visibility into a user's Internet activity."[82]

[79] *Id.* at 59-60.

[80] *See id.* at 27 (describing the role of browsers in establishing the secure connection to the website).

[81] See *Network Advertising Initiative: Understanding Online Advertising*, at http://www.networkadvertising.org/faq (last visited May 21, 2016).

[82] *Online Privacy and ISPs* at 88.

SOCIAL MEDIA PLATFORMS	• Track all information shared by users, including essentially all the information that the Commission intends to "protect" under its proposed regime. • For example, as of April 2012, Facebook collected and stored over 50 categories of data about its users. The categories include credit card information, phone numbers, real-time activities information (including the content of messages sent using the site, precise geolocation information tagged by time visited, and information about the devices used to access Facebook).[83] Today, Facebook collects even more information, including metadata about things like app usage and data collected through technologies such as facial recognition software,[84] all of which can be used to compile detailed user profiles for advertising purposes. • In addition, Facebook uses its "Like" button to obtain access to a pervasive view of users' web surfing activities. When a Facebook subscriber is logged into Facebook and goes to another website with a Facebook "Like" button on it (which includes the vast majority of websites), the information Facebook receives "includes your user ID, the website you're visiting, the date and time and other browser-related info." Facebook also receives "a more limited set of info" about users of websites that contain a "Like" button even if the user is not a Facebook subscriber or is not logged in to Facebook at the time the site was visited.[85]
MOBILE APPLICATIONS	• Collect and share substantial amounts of sensitive user information, such as unique device IDs, users' email addresses and web browsing activity, bookmarks, app usage history, Wi-Fi history, call logs, geolocation information, photos, videos, and users' contact and calendar information. • "Once the mobile app has collected user data that data can provide revenue to the app developer or sold to other companies that gather information from multiple apps. . . . Many mobile apps share this customer data with third parties as a way to support offering the app for free without imposing subscription fees. The consumer data from an individual app may be aggregated with data from other apps to make it more valuable to advertisers.[86]

[83] Facebook's Data Pool – Last Location, at http://europe-v-facebook.org/EN/Data_Pool/data_pool.html#LastLocation (last visited May 21, 2016).

[84] *Online Privacy and ISPs* at 66-80.

[85] Facebook Help Center – What information does Facebook get when I visit a site with a Like button?, at https://www.facebook.com/help/186325668085084/?q=pluginds&sid=0CnsdsFI6S0w9XwnZ (last visited May 21, 2016).

[86] *Online Privacy and ISPs* at 70; *see also* Dan Goodin, *Researchers find 256 iOS apps that collect users' personal info*, ARS TECHNICA (Oct. 19, 2015), http://arstechnica.com/security/2015/10/researchers-find-256-ios-apps-that-collect-users-personal-info/ (reporting that certain apps are able to gather information prohibited by Apple's

OPERATING SYSTEMS	• Have access to all data and programs on a device and collect significant consumer data and search terms for targeted ads. • Mobile operating systems use persistent trackers that operate across multiple apps, enabling the OS provider to track usage across the user's Internet activity.[87] • Personal assistants operating on operating systems, such as Apple's Siri, Google's Google Now, and Microsoft's Cortana also give OS providers access to significant consumer data, such as the user's calendar, search queries asked of the assistant, and other data from relevant apps.[88] • Desktop operating systems also gather significant amounts of data about the individual or individuals who use the PC. For example, the default settings for Windows 10 allows the operating system to "gather up your contacts, calendar details, text and touch input, location data, and a whole lot more. The OS then sends it all back to Microsoft so that it can be used for personalisation and targeted ads."[89]

privacy policy, including information on all of the apps installed on a user's phone, the platform serial number of the devices in certain instances, a list of the hardware components of some devices and the serial numbers of these components, the email address associated with users' Apple IDs).

[87] *Online Privacy and ISPs* at 16, 68-69.

[88] *Id.* at 66.

[89] Sebastian Anthony, *Windows 10 Doesn't Offer Much Privacy by Default: Here's How to Fix It*, ARS TECHNICA (Aug. 4, 2015), http://arstechnica.com/information-technology/2015/08/windows-10-doesnt-offer-much-privacy-by-default-heres-how-to-fix-it/.