
**Before the**

**Federal Communications Commission**

**Washington, D.C. 20554**

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

# Comments in Support of Petitions for Reconsideration and Reply to Opposition to Petitions for Reconsideration of the International Center for Law & Economics

**March 6, 2017**

## I. Introduction

"[W]e have an obligation to make certain that BIAS providers are protecting their customers' privacy while encouraging the technological and business innovation that help drive the many benefits of our increasingly Internet-based economy."[1] So begins the Order, rightfully recognizing that mandated privacy and security protections must be designed to ensure that they do not undermine the larger goals of promoting broadband innovation and encouraging broadband access and use. As the Commission recognized in the NPRM that preceded the Order, "[t]he intersection of privacy and technology is not new."[2]

And yet the Order sets out a privacy regulatory regime for 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 the application of *ex ante* privacy principles across industries is a fraught exercise as each industry — indeed each firm within an industry — faces a different set of consumer expectations about providing innovative services and privacy protections.[3] In this area, 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 Order, by contrast, eschews consideration of business realities, and adopts a more prescriptive, more invasive privacy regime that is inconsistent with "best practices" promoted by other agencies. Instead, the Order relies solely on hypothetical, *potential* harms that *could* arise, according to a small subset of comments it received that describe *not* ISPs' actual practices, but merely the extent of ISPs' potential access to personal data.[4]

Thus, for instance, the Order asserts that the ISPs' "position ***allows*** them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents."[5] And it goes on to opine that, even with encryption, "encrypted web traffic ***can be used to infer***" what pages and resources users access.[6] But when

---

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, FCC 16-148 (rel. Nov. 2, 2016), at ¶ 1[hereinafter "Order"]. Of course, it is far from clear that the Commission in fact has a *legal* basis for applying CPNI rules drafted for switched-telephone networks to modern high-speed broadband networks. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Reply Comments of TechFreedom, WC Docket 16-106 (July 6, 2016) at 7.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket 16-106 (rel. April 1, 2016), at ¶ 1[hereinafter "NPRM"].

[3] *See, e.g.*, PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES (2012), at 76 ("The basic structure of fair information practices typically applies across... sectors, but the detailed rules and practices may vary.").

[4] Order at ¶¶ 29-35.

[5] *Id.* at ¶ 30.

[6] *Id.* at ¶¶ 33-34

it comes to assessing actual practice, the Commission fails to address the actual business realities that dictate a far more circumscribed approach to ISP use of consumer data.

There are two fundamental problems with this framing. First, it is a cherry-picked, selective presentation of the state of our knowledge about ISPs' *ability to access* personal data. Second, it offers up these potentialities as foregone conclusions, asserting a need for consumer protection against the presumed depredations of prying ISPs based on mere *ability*, rather than consideration of business realities that guide their actual conduct. Those realities suggest strongly that risk of harm cannot be inferred from mere ability, do not support the FCC's opt-in approach, and counsel in favor of a case-by-case assessment of actual allegations of harm consistent with the FTC's approach, rather than a restrictive, *ex ante* rule.

## II. The Order Mischaracterizes ISPs' "Unique" Ability to Access Personal Information

The justification offered in the Order to impose special rules for ISPs rests, crucially, on the assertion that "BIAS providers are not, in fact, the same as edge providers in all relevant respects."[7] To support this claim, the Order repeatedly cites various commenters who claim that ISPs have the ability to combine consumer data and Internet usage history into a "very unique, detailed and comprehensive view of their users."[8] The FCC uses this language to make its case that ISPs' collection and use of consumer data creates unique concerns, that they should thus be regulated differently (and more onerously), and that doing so is consistent with the FTC's approach:

> While we recognize that there are other participants in the Internet ecosystem that can also see and collect consumer data, the record is clear that BIAS providers' gatekeeper position allows them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents.[9]

As we discuss below, the Order is, in fact, *inconsistent* with the FTC's approach.[10] Moreover, ISPs' access to sensitive data is not, in fact, unique, and, contrary to the Order's cherry-picked assertions, the latest comprehensive analysis suggests that ISPs' access is *more*

[7] Order at ¶ 35; *see generally* Order at ¶¶ 28-37.

[8] See, *e.g.*, *id.* at ¶ 32.

[9] *Id.* at ¶ 30.

[10] *See infra* note 37, ff.

*limited* than that of many edge providers.[11] Having "some" access is very different than having "comprehensive" access.

The Order's most basic claims are paradigmatic examples of the misleading use of statistics. First, the Order asserts that ISPs "see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents."[12] Perhaps that is true "while on *the* network," but users rarely remain on a single network, and, just as they "multi-home" between multiple edge providers, they also move between ISPs throughout the day and over time.

Moreover, despite its appendage by the Order as if an afterthought, "absent encryption" describes a small and rapidly disappearing proportion of Internet traffic.[13] The Order relies on seemingly outdated data to claim that encryption is insignificant.[14]

The Order then asserts that:

> By contrast, edge providers only see a slice of any given consumers Internet traffic. As explained in the record, edge providers' visibility into consumers' web browsing activity is necessarily limited. According to the record, only three companies (Google, Facebook, and Twitter) have third party tracking capabilities across more than 10 percent of the top one million websites, and none of those have access to more than approximately 25 percent of web pages.[15]

In truth, edge provider visibility *is*, of course, necessarily limited — but not by much. The assertion that companies like Google, Facebook and Twitter can track "no more than… 25 percent of web pages" is disturbingly misleading. The *fraction of all webpages* tracked is not the proper metric: the *share of user visits* more nearly is. For example, the top 10 websites (a miniscule fraction of the number of the total number of web pages) alone account for 33

---

[11] *See* Peter Swire, Justin Hemmings & Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Institute for Information Security & Privacy at Georgia Tech (May 2016), *available at* http://bit.ly/2lvRtsj [hereinafter "Swire, *et al.*, *Online Privacy And ISPs*"]

[12] Order at ¶ 30.

[13] In just the time since the Order was drafted, the share of "top 100" sites with HTTPS encryption by default has gone from 21 percent to almost 40 percent, and 50 percent use HTTPS, either by default or after login. *Compare HTTPS on Top Sites*, GOOGLE TRANSPARENCY REPORT (last visited Mar. 6, 2017), https://www.google.com/transparencyreport/https/grid/, *with* Brian Barrett, *Most Top Websites Still Don't Use a Basic Security Feature*, WIRED (Mar. 17, 2016), http://bit.ly/2lXLg4D. *See also* Swire, *et al.*, *Online Privacy And ISPs*, at 36 ("All of the top 10 sites… [and] 42 of the top 50 sites either use HTTPS by default or shift to HTTPS when the user logs-in…[and] 24 of the top 50 sites use HTTPS by default, even without user log-in.").

[14] *See, e.g., Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Reply Comments of Peter Swire & Justin Hemmings, WC Docket 16-106 (July 6, 2016), at 3-5.

[15] *Id.*

percent of US website visits.[16] All of these sites are tracked by (most are *owned* by, in fact) the largest online platforms, and *all* of them use encryption by default. On this measure, the ability of social media, search and e-commerce companies to track behavior and access data surely comprises an overwhelming share of the web — and not surprisingly, of course: These companies have an interest in prioritizing the tracking of the most trafficked websites.

When misleading, non-evidence "evidence" is offered as the only basis for a claim, there is reason to suspect that the actual evidence to support the contention simply doesn't exist.

Similarly, on the basis of mere unsupported assertions by commenters, the Order makes a number of claims about ISPs' allegedly exceptional ability to view consumers' data.[17] In fact, non-ISP information collection practices are frequently far more robust than those of ISPs. In Appendix A to these Comments 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 and coauthors note, "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."[18] Compared to their edge-provider analogues, ISPs do not have particularly broad insight into consumer data that is not given to them in the course of subscribing.[19]

## III. The Order Improperly Focuses on Technical Possibilities Without Considering Market Realities

To begin with, the FCC makes clear throughout the Order that its initial acknowledgement that privacy protections and innovation may be at odds was an empty one. Instead, the FCC falls back on the faulty logic of the Open Internet Order's "virtuous circle" to claim, in effect, that only regulation can preserve the Internet's immense success:

> The risk of privacy harms directly affects behavior and activity by eroding trust in and use of communications networks. As the Commission has found, if "consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access

[16] *Most popular websites in the United States as of February 2016, based on share of visits*, STATISTA (last visited Mar. 6, 2017), http://bit.ly/2lTVXoR (based on calculations during the week ending February 27, 2016).

[17] *See, e.g.,* Order at n. 56, ¶ 29, and ¶ 33.

[18] Swire, *et al.*, *Online Privacy And ISPs*, at 7.

[19] *See id.* at 23.

> services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand."[20]

In a microcosm of the poverty of the "virtuous circle" theory, that section of the Open Internet Order, in turn, cites to a Pew study that claims that, of the 15 percent of American adults who didn't use the Internet in 2013, three percent pointed to "worried about privacy" as their main reason for not doing so.[21] Six percent, however, pointed to "too expensive" as their main reason[22] — something that can only be *exacerbated* by the Order. The notion that mitigating (in theory) a problem impeding three percent of users while exacerbating a problem that impedes six percent will *increase* consumer demand is an absurd one, of course.

Further emblematic of the Order's lack of careful analysis, the Order asserts that "requiring opt-in approval for the use and sharing of sensitive customer PI reasonably balances burdens between carriers and their customers."[23] Yet this assertion is made without pointing to any cost-benefit analysis indicating whether, as an *ex ante* rule, it makes sense in every case to impose notice requirements between ISPs and consumers. To point out just one problem with this approach, it is well known in the literature that consumers often suffer from "information overload"[24] such that it will not always be frictionless — or, on net, helpful — for consumers to be aware of the "costs and benefits of participation in these programs." Instead, in many cases, consumers will evaluate the services of ISPs *as a whole*, treating their privacy — which for different consumers will have a different value — as just one component of their relationship with an ISP which includes, among other things, convenience, overall cost, speed, and reliability.

Moreover, the Order will 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,

---

[20] Order at ¶ 380 (quoting *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5821, ¶ 464 (2015)).

[21] Pew Research Center, *Who's not online and why* (Sep. 2013), at 2, *available at* http://pewrsr.ch/2lO0gks.

[22] *Id.*

[23] Order at ¶ 193.

[24] *See, e.g.,* Troy A. Paredes, *Blinded by the Light: Information Overload and Its Consequences for Securities Regulation*, 81 WASH. U. L. Q. 417 (2003).

and services for free,[25] and don't care much about privacy except with respect to the most sensitive information (e.g., healthcare data, children's educational records),[26] so long as the personal data they provide is secure and they get something of value in return.[27] The FCC's prescriptive and onerous rules simply do not address the heterogeneity of consumer preference and its effect on these markets.

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

The artificial bifurcation of the market between BIAS and edge providers betrays the Order's ignorance of market realities. In the truly relevant market — the market for advertising and data analytics — the distinction between edge and network is unimportant, and competition abounds. The paucity of evidence and analysis of the competitive dynamics of the advertising and broader informatics markets in the Order is fatal to its proposed approach.

In fact, the Order addresses potential ISP use of data-sharing in exchange for consumer discounts in a mere six paragraphs,[28] inexplicably adopting "heightened disclosure and choice requirements" (including opt-in consent)[29] that are at squarely odds with the FTC's approach in such circumstances.[30]

The Commission asserts that ISP competition (in the BIAS market) is insufficient to protect consumers: "While some customers can switch BIAS providers…, "[b]roadband providers have the ability to act as gatekeepers even in the absence of 'the sort of market

---

[25] *See, e.g.*, Mary Ellen Gordon, The History of App Pricing, and Why Most Apps are Free, The Flurry Blog (Jul. 18, 2013), http://bit.ly/2muGBdn.

[26] Thus certain sector-specific privacy regimes do impose opt-in requirements in certain cases. *See, e.g.,* 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 is decidedly not of this sort.

[27] *See, e.g.*, 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.

[28] Order at ¶ 298-303.

[29] *Id.* at ¶ 301.

[30] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106 (May 27, 2016), at 3 (noting the inconsistency and further noting that "the [FTC Privacy Report] observed [that] 'big data can create opportunities for low-income and under-served communities,' and cites a broad range of existing examples"). The Order briefly acknowledges possible benefits but then adopts its "heightened" approach based solely on the *possibility* that the practice *may* present "possible benefits and harms." Order at ¶ 301.

concentration that would enable them to impose substantial price increases on end users.'"[31] But there is little indication that broadband access is lacking adequate competition, and strong indications that both current access and future broadband development will ensure sufficient competition to protect privacy-sensitive consumers — assuming there are in fact enough of them to justify the cost of ISPs adopting different access models at all.[32]

More important, ISPs face daunting competition in advertising markets. Within the advertising market, ISPs do not have access to any greater amount of useful consumer data — and possibly quite a bit less — than any other actor. Yet the Commission asserts that, unlike edge providers, ISPs "can collect 'an unprecedented breadth' of electronic personal information"[33] — an assertion made without citing to any sort of economic (or other) analysis to justify its conclusion. Thanks to healthy competition in the broader advertising market, however, a wide range of companies do in fact have access to copious amounts of useful data.

Compared to ISPs, the scope of data available to edge providers is truly pervasive, allowing them to gather data on users across devices and contexts.[34] All of these companies, including ISPs, have the ability to collect and use consumer data. But they are limited by the market dynamics that constrain them, including from interactions with each other.

Of crucial importance (and completely ignored by the Order), it is not enough to have *access* to data; rather, it must be competitively valuable in order to make its collection and processing worthwhile. But "ISPs in many instances have access to data that is less revealing than content or other information about user activity available to the companies providing services to the user."[35] While ISP data may, in some cases, be unique, it is not generally

---

[31] Order at ¶ 36 (citations omitted). *See also, e.g.*, Open Technology Institute, *The FCC's Role in Protecting Online Privacy: An Explainer* (Jan. 2016) at 2-3 (characterizing ISP's as "gatekeepers" that "face little competition"), *available at* http://bit.ly/2lNRDXa.

[32] *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable & Timely Fashion, & Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, 30 F.C.C. Rcd. 1375 ¶ 83 (2015). The Commission, of course, changed the threshold for "broadband" access to 25 Mbps download speed in 2015, instantly wiping out some of this competition (on paper). But, presumably, for privacy-sensitive consumers, the possibility of a more protective ISP even at slightly slower speeds (in any case, well above those needed for the vast majority of Internet uses) would make 10 Mbps and 25 Mbps networks more directly competitive. Meanwhile, over 93% of consumers have access to at least three mobile broadband providers. *See In re Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993: Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Seventeenth Report*, 29 F.C.C. Rcd. 15311 ¶ 51, Chart III.A.2 (2014).

[33] Order at ¶ 28.

[34] *See, e.g., Facebook Exchange*, FACEBOOK BUSINESS (last accessed Jul. 5, 2016), *available at* http://bit.ly/2mutoRO; Marcelo Ballvé and Emily Adler, *The Atlas Explainer: Where Facebook's Atlas ad server fits in the digital-ad ecosystem, and how it works*, BI INTELLIGENCE (Apr. 10, 2015) *available at* http://read.bi/2muwup2.

[35] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Reply Comments of Peter Swire & Justin Hemmings, WC Docket 16-106 (July 6, 2016), at 9.

uniquely valuable, and thus competitive pressures may deter ISPs from expending resources to access and process it in the first place. And unless ISPs can replicate the benefits derived from the highly valuable data that edge providers gather, advertisers have no reason to favor ISPs over current, dominant networks. Far from being juggernauts of potential ad sales, ISPs are much more like new entrants that bring innovative competition to the advertising marketplace — but are also more likely than not to fail.

Moreover, to the extent that "sufficient competition" is a touchstone for adequate privacy protection, the Commission has not actually evaluated the extent of competition in the relevant markets, nor actually determined whether ISPs face more or less competition along the relevant dimensions than do, say, Google and Amazon.[36]

It is incumbent upon proponents of privacy regulation, and especially *differential* regulation, to justify any particular proposed regime with evidence that demonstrates that consumer privacy, consumer welfare, and the public interest will be served. The Order fails to do so.[37]

### B. The Order's opt-in requirement fails to account for business realities that suggest it will do more harm than good

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 Order also fails to justify the specific rules it prescribes. Of greatest significance is the imposition of an opt-in requirement for the sharing of sensitive data.

The Commission asserts that this rule is needed because

> [a]s the FTC recognizes, "the more sensitive the data, the more consumers expect it to be protected and the less they expect it to be used and shared without their consent." We therefore require BIAS providers and other telecommunications carriers to obtain a customer's opt-in consent before using, disclosing, or permitting access to his or her sensitive customer PI… We anticipate that this will increase the amount of clear and informative information that customers will have about the costs and benefits of participation in these programs.[38]

But these assertions completely miss the point that more consumer disclosures do not necessarily empower consumers. And, more important, the mere fact that a consumer's information may be used in ways that the user doesn't expect or understand does not mean

---

[36] *See generally* Swire, *et al.*, *Online Privacy and ISPs*.

[37] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Comments of the International Center for Law & Economics and Scholars of Law & Economics, WC Docket 16-106 (May 27, 2016).

[38] Order at ¶¶ 192-93.

that such use is harmful to consumers individually or in the aggregate. Whether such uses are on net beneficial or harmful to consumers, and whether any particular form of consent is optimal, are empirical questions — ones that have been extensively researched (although not in the Order). And in the end, "'[o]pt-in' provides no greater privacy protection than 'opt-out' but imposes significantly higher costs with dramatically different legal and economic implications."[39]

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.[40] 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: "[R]ather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive…. [I]n some cases where entry had been profitable without regulation, [some firms] will choose not to enter."[41] On net opt-in regimes may tend to favor the status quo, and to maintain or grow the position of a few dominant firms.

Thus, 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 has no basis for imposing such a potentially harmful regime on broadband and data markets. Nevertheless, the Order imposes an opt-in requirement, merely *acknowledging* that opt-in may impose more cost, but never adequately addressing the trade-offs.[42]

---

[39] *See* Fred H. Cate & Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In"* (2003), at 1, *available at* http://bit.ly/2lvZ9uz ("[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."). *See also* Nicklas Lundblad and Betsy Masiello, *Opt-in Dystopias*, SCRIPTED (2010), *available at* http://bit.ly/2lvKy2s.

[40] *Id.* at 5 ("[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.") (emphasis in original).

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

[42] Order at ¶ 386 ("Although we recognize that opt-in imposes additional costs, we find that opt-in is warranted to maximize opportunities for informed choice about sensitive information.")

### C. The Order deviates from the FTC's approach to privacy

In this way (as in others), the Order deviates from the FTC's data privacy regime. The FTC's 2012 Privacy Report, upon which the Order purports to rely as a guide for its rules,[43] tempers its concern that ISPs' have an exceptional ability to collect information, noting, with a nuance lacking in the Order, 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.[44]

Taken as whole, the FTC's 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.[45]

Rather than adopt the standards enforced by the FTC under Sections 5(a) and (n) of the FTC Act, import the FTC's Unfairness Policy Statement, and commit to the FTC's case-by-case approach to privacy enforcement, 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,"[46] and a prescriptive regime that pays lip service to such standards but imposes aggressive constraints that fundamentally limit competition and choice.

---

[43] *Id.* at ¶ 9 ("In adopting rules governing customer choice, we look to the best practices framework recommended by the FTC in its 2012 Privacy Report as well as the choice framework in the Administration's CPBR and adopt a framework that provides heightened protections for sensitive customer information.")

[44] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) at 56, *available at* http://go.usa.gov/csYRz (emphasis added) [hereinafter FTC Privacy Report].

[45] *Id. See also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Letter of Jon Leibowitz to the FCC, WC Docket No. 16-106 (May 23, 2016), at 7.

[46] Order at ¶ 5.

# 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.<br>• 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."[1]<br>• 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.[2] 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."[3] |
| **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.<br>• The intensive use of search engines enables search engine providers to collect highly specific and personalized data.[4]<br>• "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."[5] |

[1] Swire, *et al., Online Privacy and ISPs*, at 97.

[2] October 2012 Web Privacy Census (Version 2.0), http://bit.ly/2lvW3Xm (last visited Mar. 6, 2017).

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

[4] Swire, *et al., Online Privacy and ISPs*, at 51.

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

| | |
|---|---|
| **WEBMAIL AND MESSAGING** | • Scan email content as well as metadata, such as email addresses, time, date, and file size.<br>• 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.[6] |
| **BROWSERS, INTERNET VIDEO** | • Track users' information and web activity through telemetry, cookies, integrating search with other functionality, and other techniques.<br>• 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.[7]<br>• 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.<br>• 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.[8]<br>• 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."[9] |

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

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

[8] *See Network Advertising Initiative: Understanding Online Advertising*, at http://www.networkadvertising.org/faq (last visited Mar. 6, 2017).

[9] Swire, *et al., 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.<br>• 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).[10] Today, Facebook collects even more information, including metadata about things like app usage and data collected through technologies such as facial recognition software,[11] all of which can be used to compile detailed user profiles for advertising purposes.<br>• 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.[12] |
| **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.<br>• "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.[13] |

[10] *Facebook's Data Pool – Last Location*, http://bit.ly/2lXvWoJ (last visited Mar. 6, 2017).

[11] Swire, *et al., Online Privacy and ISPs*, at 66-80.

[12] *Facebook Help Center – What information does Facebook get when I visit a site with a Like button?*, http://bit.ly/2lXue6J (last visited Mar. 6, 2017).

[13] Swire, *et al., 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://bit.ly/2lXr9Ud (reporting that certain apps are able to gather information prohibited by Apple's 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).

| | |
|---|---|
| **OPERATING SYSTEMS** | • Have access to all data and programs on a device and collect significant consumer data and search terms for targeted ads.<br>• Mobile operating systems use persistent trackers that operate across multiple apps, enabling the OS provider to track usage across the user's Internet activity.[14]<br>• 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.[15]<br>• 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 allow 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."[16] |

[14] Swire, *et al., Online Privacy and ISPs*, at 16, 68-69.

[15] *Id*. at 66.

[16] Sebastian Anthony, *Windows 10 Doesn't Offer Much Privacy by Default: Here's How to Fix It*, ARS TECHNICA (Aug. 4, 2015), http://bit.ly/2lW3mUt.