TECHNOLOGY POLICY INSTITUTE
Studying the Global Information Economy

An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking

May 2016

Thomas Lenard and Scott Wallsten

1099 NEW YORK AVE, NW ▫ SUITE 520 ▫ WASHINGTON, DC 20001
PHONE: 202.828.4405 ▫ E-MAIL: info@techpolicyinstitute.org ▫ WEB: www.techpolicyinstitute.org

An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking

Thomas Lenard and Scott Wallsten[*]

May 25, 2016

[*] President and Senior Fellow, and Vice President for Research and Senior Fellow, respectively, at the Technology Policy Institute. The views reflected here are our own and do not necessarily reflect those of TPI, its staff, or its board of directors.

Table of Contents

Executive Summary

- The key question the FCC should ask in its NPRM is whether the privacy rules it proposes for ISPs would yield net incremental benefits beyond those that previously covered ISPs under the FTC. The Commission does not address this fundamental question.

- The NPRM does not acknowledge the benefits that flow from information use, including from the ability to combine and use datasets in novel ways—benefits that would decrease significantly under an opt-in regime or one that requires consent for each new use of data. At a minimum, the FCC should recognize the tradeoff between increased privacy protection and decreased benefits from data use. If it does not acknowledge the tradeoff, it cannot make an informed decision.

- The Commission provides no support for its claim that ISPs necessarily have access to more, and more sensitive, data than do edge companies. An increasing share of traffic that is encrypted—across the board, but especially in the finance and health care sectors, areas in which consumers worry about privacy the most—use of VPNs, and other anonymizers are steadily decreasing whatever view ISPs do have of online behavior. Moreover, more than 80 percent of internet users report using the internet at multiple locations even as they continue to use the same search, social, and email accounts, meaning that any given ISP is unlikely to have a complete view of browsing behavior even without encryption.

- Data show little, if any, link between privacy concerns and broadband adoption. In the July 2015 Current Population Survey Computer (CPS) and Internet Use Supplement survey less than one-half of one percent of internet non-adopters report privacy concerns as the primary reason for not subscribing. Moreover, even if this claim were true it would apply also to edge companies.

- Treating ISPs differently from edge companies would put ISPs at a competitive disadvantage in the large and growing digital advertising market, which had revenues of approximately $60 billion in 2015. This disadvantage would pose an entry barrier to ISPs, denying them a source of revenues and therefore helping to ensure that they continue to cover all their costs from direct payment by end users. It could also prevent new ISPs from using advertising—the go-to funding source for many edge companies — to offset consumer prices. Some ISPs are, in fact, trying that model. Additionally, blocking entry into the digital advertising market may harm any firm that needs to advertise as part of its business, since they will have fewer options on where they can advertise.

Introduction

The Federal Communications Commission (FCC) recent Notice of Proposed Rulemaking (NPRM) proposes privacy rules for Broadband Internet Access Service (BIAS) providers—also known as Internet Service Providers (ISPs)—that would be stricter than the standards that apply to edge providers and other companies under the jurisdiction of the Federal Trade Commission (FTC).[1] The NPRM begins with a warning from Warren and Brandeis's 1890 treatise on privacy: that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet should be proclaimed from the house-tops.'"[2] However, the FCC should consider Warren and Brandeis's statement later in the treatise that "It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[3]

The "purpose" of their article is particularly relevant for this NPRM. Given the enforcement regime already developed and implemented by the FTC, the FCC should begin by asking whether "existing law…can be properly invoked to protect the privacy of the individual." The FTC does not have jurisdiction over common carrier services, so it may be true, as the Commission claims, that no existing law explicitly covers privacy with respect to ISPs.[4] Nevertheless, the FCC should consider whether the new privacy rules the NPRM proposes would yield net benefits relative to the FTC's approach.

As discussed below, the FTC has decades of experience considering privacy tradeoffs and enforcing consumer privacy standards. In the current era of big data and online privacy concerns, the FTC has hosted workshops, issued reports, and engaged in enforcement actions against internet companies and ISPs. The FCC, by contrast, does not appear to have considered these tradeoffs at all. It cites its experience limiting "incumbent telephone companies' use and sharing of customer information"[5] and its work on Customary Proprietary Network Information (CPNI) rules[6] as evidence of its competence in regulating privacy and data security online.

The FCC hosted one workshop on broadband consumer privacy in April 2015.[7] The workshop featured 12 privacy experts, plus FCC staff as panel moderators, who offered a variety of opinions reflecting the complex nature of the issue. Unfortunately, the NPRM does not discuss or cite the workshop.

Instead, the FCC begins by implicitly assuming that the privacy regime under which ISPs have been governed was not sufficient and that it must craft a new one. The FCC argues that stricter controls are warranted because ISPs have a clearer view of private information than anyone else

[1] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," Notice of Proposed Rulemaking, (March 31, 2016).
[2] Ibid., para. 1.
[3] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1890).
[4] As non-lawyers, we take no position on which laws apply and how.
[5] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 6.
[6] Ibid., para. 7.
[7] https://www.fcc.gov/news-events/events/2015/04/public-workshop-on-broadband-consumer-privacy

in the internet ecosystem. Even if we were to accept that argument—which is dubious at best, as discussed below—the FCC should still demonstrate that its proposed stricter rules would lead to net incremental benefits beyond those under the FTC's approach. It should also analyze the potential the implications of adopting one set of rules for ISPs while other parts of the internet ecosystem remain governed by FTC standards. It does neither.

The remainder of this paper discusses the value of information in the digital economy, the FTC's experience with privacy protection, why it is not sensible to treat ISPs differently than edge providers, and problems and questions regarding the FCC's specific proposals.

The Value of Information

The NPRM focuses solely on reducing personal information available for use by ISPs without acknowledging how important that data has been for the development of the internet. Any rule that restricts the use of information represents a tradeoff between the benefits of increased privacy and the cost of decreased information in the marketplace.[8] The NPRM does not acknowledge this tradeoff, let alone the possibility that the costs of its rules could potentially outweigh the benefits. This section discusses the benefits of information, which could be diminished or lost under the FCC's proposal.

Advertising revenues—and targeted advertising in particular—have played a key role in supporting new online services, which are often provided to consumers free of charge. Perhaps the most prominent example is the search engine, which would likely not exist as we know it were it not for the ability of Google and others to develop new sources of revenue based on targeted advertising.

Advertising is not companies' only use of customer data. It is also used to develop new products and services that consumers are likely to value. Netflix, for example, uses viewing data to inform its development of original content.[9] Data can also be used to improve algorithms, protect against security threats, and notify buyers of a product of important recalls, to name but a few.

As the use of "big data," has become more common, the broader societal value of online data is increasing.[10] The President's Council of Advisors on Science and Technology (PCAST) noted in a report on big data that "[t]he beneficial uses of near-ubiquitous data collection are large, and they fuel an increasingly important set of economic activities."[11] The World Economic Forum noted that data can be used to make financial services more inclusive, improve education, expand

---

[8] See, generally, Thomas M. Lenard and Paul H. Rubin, "In Defense of Data: Information and the Costs of Privacy," *Policy & Internet* 2, no. 1 (January 15, 2010): 143–77, doi:10.2202/1944-2866.1035.

[9] David Carr, "Giving Viewers What They Want," *The New York Times*, February 24, 2013, http://www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html.

[10] Thomas M. Lenard and Paul H. Rubin, "Big Data, Privacy, and the Familiar Solutions" (Technology Policy Institute Working Paper, May 2014).

[11] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective," May 2014, x, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

health coverage, and improve agricultural productivity.[12] The McKinsey Global Institute described additional potential benefits in health care, government services, fraud protection retailing and manufacturing.[13] A 2014 White House report on big data observes that "properly implemented, big data will become an historic driver of progress."[14]

Many of these benefits come when data can be reused, combined with other data sets, and used to answer new questions that were not anticipated at the time the data was collected.[15] Innovations often come from using multiple sources of data, which may include transferring data to third parties. That approach can enhance the value of data for purposes ranging from epidemiology studies to marketing.[16] Eliminating the "option value" of future use and serendipitous results makes any data less valuable.

As such, rules that limit data collection and use must be considered carefully to avoid imposing large costs on innovation and the economy. As the PCAST Report notes, "a policy focus on limiting data collection will not be a broadly applicable or scalable strategy—nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth)."[17]

The information economy, as its name implies, thrives on information. Few question the importance of privacy protections, but rules that restrict the use of information must carefully assess whether those rules generate any benefits and, if so, whether those benefits outweigh the potential harms.

---

[12] The World Economic Forum, "Big Data, Big Impact," 2012, http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf.

[13] McKinsey Global Institute, "Big Data: The next Frontier for Innovation, Competition, and Productivity," May 2011.

[14] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values," May 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[15] Over the past few weeks we have struggled, as we imagine others writing comments have, with the question of whether data should be considered singular or plural. We know that it is the plural of datum. We both tend to use it that way. In this report, however, we decided to follow the precedent in FiveThirtyEight and pretend it is singular. http://fivethirtyeight.com/datalab/data-is-vs-data-are/

[16] Simple examples of unexpected uses of data exist, as well. The Centers for Disease Control (CDC) conducts an annual health survey—the National Health Information Survey. The CDC notes that the survey "is the principal source of information on the health of the civilian noninstitutionalized population of the United States and is one of the major data collection programs of the National Center for Health Statistics (NCHS) which is part of the Centers for Disease Control and Prevention (CDC). The National Health Survey Act of 1956 provided for a continuing survey and special studies to secure accurate and current statistical information on the amount, distribution, and effects of illness and disability in the United States and the services rendered for or because of such conditions."[16.1] Among many topics one would expect of a health survey, it also asks about household wireless telephony use. As a result, the CDC data has become the leading source of information about the prevalence of wireless-only households. Moreover, because the survey has demographic information, we also know that lower-income households are more likely to be wireless only. Neither the CDC nor the survey participants were likely to know that their data would be used in this way, but it has become a key input into telecommunications policy decisionmaking.

[16.1] http://www.cdc.gov/nchs/nhis/about_nhis.htm

[17] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective," x–xi.

Do ISPs Require Stricter Privacy and Data Breach Rules than Edge Providers?

The FTC has been considering the tradeoff between the value of data and privacy concerns for decades, noting that it "has been the chief federal agency on privacy policy and enforcement since the1970s, when it began enforcing one of the first federal privacy laws – the Fair Credit Reporting Act."[18] The FTC has taken this role seriously with respect to the digital economy, issuing papers, hosting workshops, establishing rules and guidelines, and enforcement actions.[19] Table 1 presents an abridged list of recent FTC activities on privacy and data security.

Table 1: FTC Privacy and Data Security Activities, Abridged List

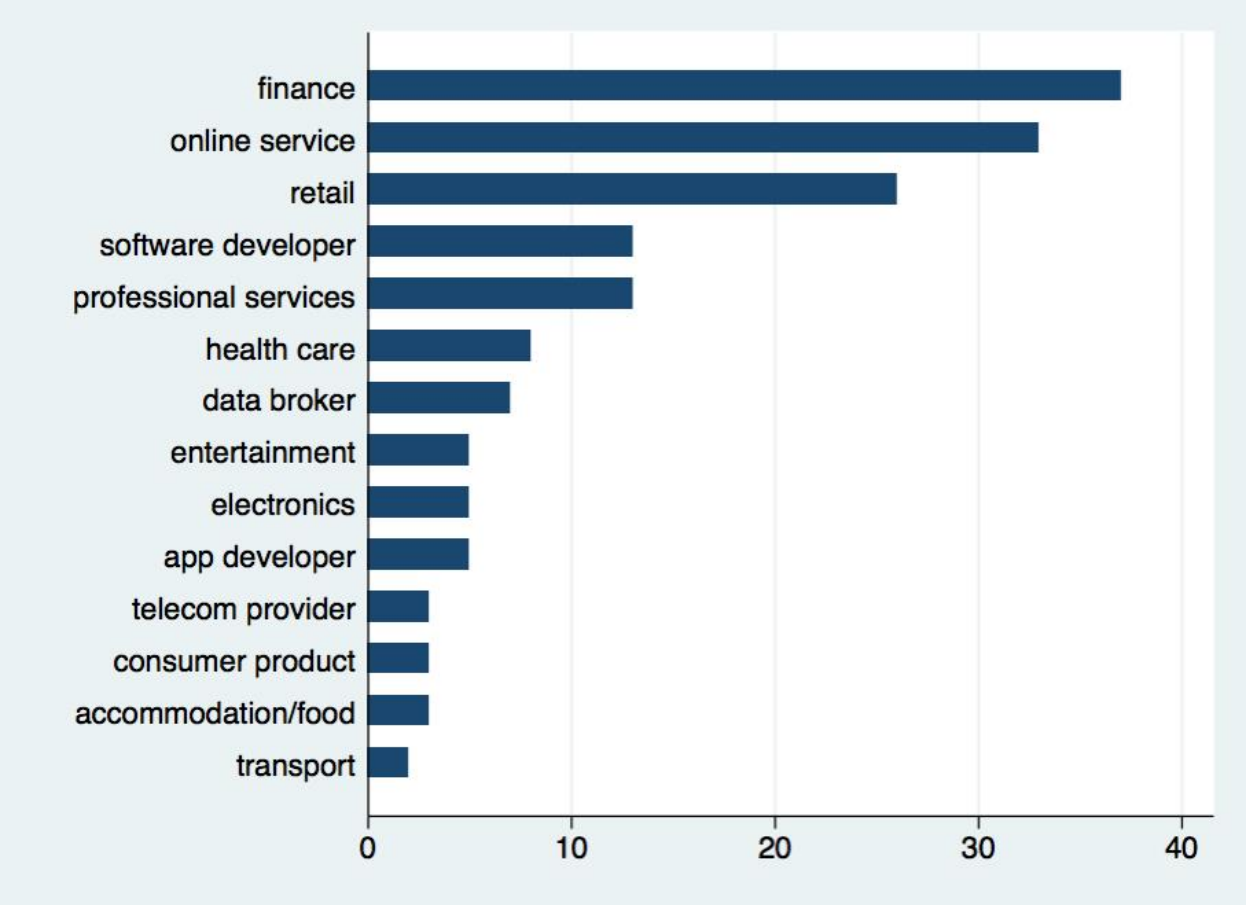
Type of Activity and Title	**Date**
Events and Workshops	
Start with Security Chicago	15-Jun-16
Start with Security Seattle	9-Feb-16
PrivacyCon	14-Jan-16
Cross-Device Tracking Workshop	16-Nov-15
Start with Security Austin	5-Nov-15
Big Data: A Tool for Inclusion or Exclusion?	15-Sep-15
Start with Security San Francisco	9-Sep-15
Internet of Things Workshop	19-Nov-13
Workshop on Facial Recognition Technology	8-Dec-11
Exploring Privacy: A Roundtable Series	17-Mar-10
Exploring Privacy: A Roundtable Series	28-Jan-10
Exploring Privacy: A Roundtable Series	7-Dec-09
Guidance and Rules	
Privacy of Consumer Financial Information (Financial Privacy Rule)	May 24, 2000 (Amended June 24, 2015)
Children's Online Privacy Protection Rule	April 27, 1999; most recently amended August 7, 2015
Guidance for Developers of Mobile Health Apps	5-Apr-16
Red Flags Rule	11-Feb-13
Health Breach Notification Rule	29-Aug-09
Standards for Safeguarding Customer Information (Safeguards Rule)	23-May-02
Reports	
Recommendations to Business on Growing Use of Big Data	6-Jan-16
Internet of Things: Privacy and Security in a Connected World	Jan-15

[18] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy
[19] The FTC's activities from 2015 alone can be found here: https://www.ftc.gov/reports/privacy-data-security-update-2015

Data Brokers: A Call for Transparency and Accountability	May-14
Protecting Consumer Privacy in an Era of Rapid Change	Mar-12
Protecting Consumer Privacy in an Era of Rapid Change (preliminary report)	Dec-10

The FTC, moreover, has not been shy about bringing enforcement actions against companies that violate consumer privacy or suffer from data breaches. As FTC Commissioner Maureen Ohlhausen observed in a recent speech, "We have brought more than 150 privacy and data security related enforcement actions, including actions against ISPs and against some of the biggest companies in the internet ecosystem. We also conduct extensive consumer and business outreach and guidance, coordinate workshops to foster discussions about privacy in emerging areas, coordinate on privacy efforts internationally, and advocate for policies about privacy and data use that improve consumer welfare."[20] Indeed, we count 155 FTC enforcement actions across a wide range of industries the FTC tags as "privacy and security" or "consumer privacy" (Figure 1).

Figure 1: FTC Actions tagged Privacy or Privacy and Security, 2005-2015



Source: Derived from FTC.[21]

[20] Maureen Ohlhausen, "The FTC, The FCC, and BIAS," 2016, https://www.ftc.gov/system/files/documents/public_statements/942823/160331gmuspeech1.pdf.
[21] Enforcement actions tagged "privacy and security" available here:

To be sure, some have criticized FTC rules and reports.[22] Regardless, the FTC has spent years thinking, gathering public and expert feedback, and issuing rules on privacy and data security issues.

The FCC argues that the FTC's enforcement is not sufficient, and that ISPs require special attention:

> because 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. Indeed, the whole purpose of the customer-provider relationship is that the network becomes an essential means of communications with destinations chosen by the customer; which means that, absent 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.[23]

The NPRM implies that the FTC agrees with this point of view, quoting from the FTC's 2012 Consumer Privacy Report: "…as the FTC has explained, 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."[24] However, that was not the FTC's conclusion. To the contrary, the following paragraph of that FTC report noted:

> At the same time, the Commission agrees that any privacy framework should be technology 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. Consumers, moreover, might have limited ability to block or control such tracking except by changing their operating system or browser. Thus, comprehensive tracking by any such large platform provider may raise serious privacy concerns.[25]

In other words, the FTC considers ISPs just one of many "large platform" providers potentially with access to sensitive data and appears to argue that they should not be treated differently.

The NPRM itself notes, "The importance of privacy protection is certainly not new to the nation's largest broadband providers, all of which have publicly available privacy policies, describing their use and sharing of confidential customer information. Beyond the policies, many broadband providers have chief privacy officers, and together with their staffs and colleagues,

---

https://www.ftc.gov/taxonomy/term/245/type/case; actions tagged "consumer privacy" available here: https://www.ftc.gov/taxonomy/term/247/type/case. Brandon Silberstein, TPI research associate extraordinaire, tabulated these by industry, year, type of violation, and amount paid as a fine or settlement.

[22] One of us, in particular, has been an occasional critic. See, for example, Thomas M. Lenard, "Comments Regarding FTC Report, Protecting Consumer Privacy in an Era of Rapid Change" (Technology Policy Institute, February 16, 2011), http://www.techpolicyinstitute.org/files/lenard_ftcprivacycomments.pdf.

[23] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 4.

[24] Ibid.

[25] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," Preliminary FTC Staff Report, (December 10, 2010), 56, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

they work to improve their companies' abilities to inform consumers of privacy practices, provide consumers with meaningful opportunities to control consumers' own data, and ward off attempts to breach the security of their broadband networks"[26]

Nonetheless, the FCC believes "the current federal privacy regime, including the important leadership of the FTC … does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks."[27] The Commission goes on to assert that "both consumers and Internet Service Providers (ISPs) would benefit from additional, concrete guidance explaining the privacy responsibilities created by the Communications Act."[28]

However, the NPRM provides no evidence of harms or potential harms to ISP users that the current combination of market incentives and regulatory enforcement by the FTC have not satisfactorily addressed. Similarly, it provides no evidence or analysis to support this assertion and how its approach would produce benefits, let alone net benefits, relative to the status quo.

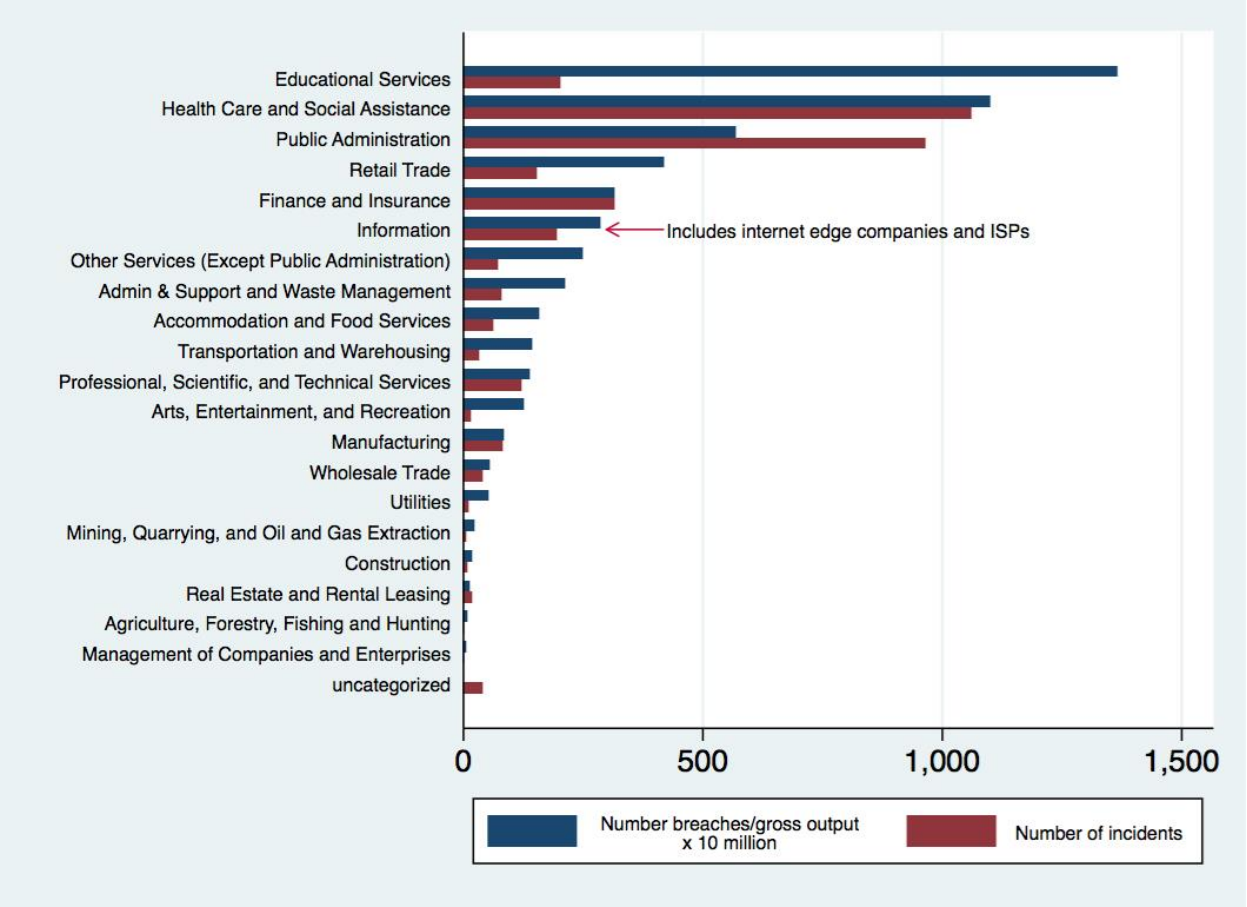
The remainder of this section discusses specific reasons why ISPs should not be treated differently from other parts of the internet ecosystem.

Data Breaches by Industry

One reason to target a particular industry might be if it has been particularly prone to damaging data breaches. Available information suggests that ISPs are no worse—and better than—several other industries. Figure 2 shows the number of data breaches by industry between 2010 and 2015 by two-digit NAICS industry code, as tabulated from the Veris Community Database (VCDB),[29] as well as the number of data breaches normalized by each industry's gross output.[30] The figure shows health care organizations and government to have suffered the most data breaches, followed distantly by finance, and finally by information and education services, which suffered an equal number of data breaches. The normalized data change the order a bit, with educational services at the top due to relatively low gross output. The industry classified as "information services" includes ISPs and edge companies like search and social media, and is fifth on this list whether normalized or not.

[26] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 10.
[27] Ibid., para. 2.
[28] Ibid.
[29] The Veris Community Database, or VCDB, describes itself as "a community data initiative to catalog security incidents in the public domain using the VERIS framework. The database contains raw data for thousands of security incidents shared under a creative commons license." http://vcdb.org/
[30] It is actually normalized by gross output 2010-2014 rather than 2010-2015 because 2015 data at the 3-digit NAICS level had not yet been published, and we wanted to make the 2-digit and 3-digit figures comparable.

Figure 2: Data Breaches by Industry, 2010-2015



Source: 2-Digit Industry Classification, VCDB;[31] Normalized by gross output per 2-digit industry (times 10 million for scale).[32]

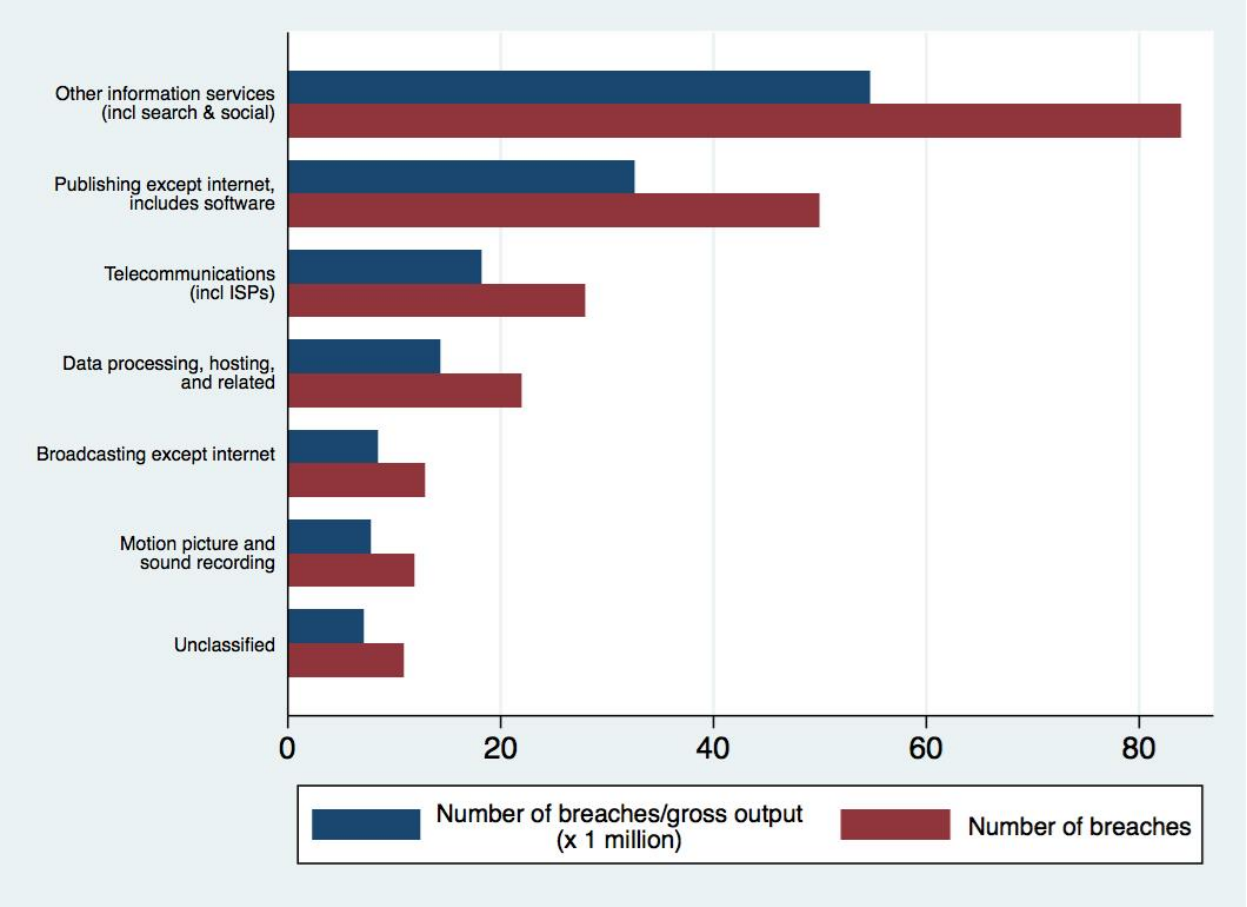
It is also possible to look in more detail at the "information services" industry. Figure 3 shows the number of data breaches by the more granular three-digit NAICS code within information services. "Other information services," which includes edge companies, has the highest number of breaches within information services, followed "Publishing, except internet, including software,"[33] and telecommunications, which includes ISPs, is third.

[31] http://vcdb.org/

[32] Normalized by gross output 2010-2014 instead of through 2015 because 2015 data was not yet available at the 3-digit NAICS level and we wanted this figure to be comparable to Figure 3. http://www.bea.gov/industry/gdpbyind_data.htm

[33] "Publishing, except internet" includes online gaming companies, which account for the majority of data breaches in that subsector.

Figure 3: Data Breaches Within Information Services, 2010-2015



Source: VCDB, subsectors within NAICS 51;[34] Normalized by gross output per 2-digit industry (times 1 million for scale).[35]

The data shows that industries classified broadly as information services are not the most frequent victims of data breaches. Moreover, even within information services, ISPs have not suffered the most data breaches. At least in terms of frequency, the data does not support a more rigorous focus on ISPs.[36]

Frequency of data breach, however, is only part of the story. The number and type of records involved also matter, as discussed in more detail below.[37] Unfortunately, the number of records

[34] http://vcdb.org/

[35] Normalized by gross output 2010-2014 instead of through 2015 because 2015 data was not yet available at the 3-digit NAICS level and we wanted this figure to be comparable to Figure 3. http://www.bea.gov/industry/gdpbyind_data.htm

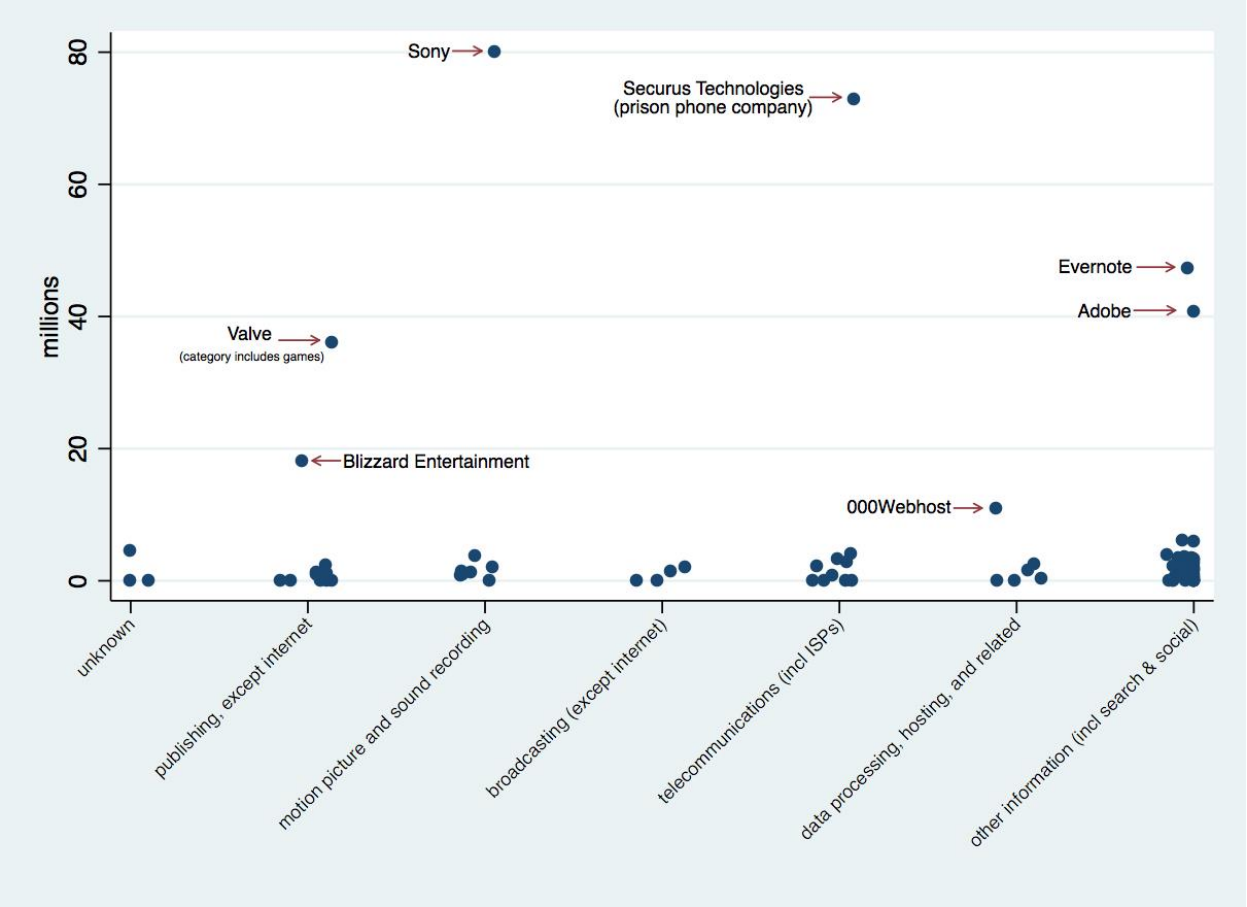
[36] The largest number of records involved in a single data breach in this dataset is the discovery of the public availability of 191 million records from voter registration lists. This breach was not classified under a particular industry in the database because it was not clear, at least at the time the data were entered, who was responsible. That data, however, appeared to be publicly available anyway. https://www.campaignsandelections.com/campaign-insider/new-leak-again-shines-light-on-data-vendors; http://www.wired.com/2015/12/reams-of-us-voter-info-appear-to-be-just-sitting-online/

[37] It is not always simple to classify the losses. The VCDB data entry instructions acknowledge as much: "This [loss categorization] is admittedly a bit confusing as documented above. Basically, the user should be able to select all

involved or the estimated severity of the breach are not consistently included in the data. For example, of the 220 data breaches counted in "information services," only 75 include the number of records involved.

Figure 4 shows the number of records involved in data breaches for the sub-industries that comprise "information services" and have data available. The largest telecommunications breach was of Securus Technologies, which had 70 million records exposed.[38] Securus is not an ISP—it provides telephone service to prisons. Among ISPs, the largest data breach tabulated here was Verizon Enterprise Solutions, with three million records exposed. Among edge companies, the largest breaches were Evernote with 50 million records and Adobe with 38 million records.

Figure 4: Number of Records Involved in Data Breach in Information Services 2010-2015



Source: VCDB, subsectors within NAICS 51[39]

varieties of losses that apply and then be able to provide a relative rating (minor, moderate, major) and/or a quantitative estimate ($) of losses for each variety selected. Furthermore, we allow a triangular distribution (expected, min, max) to be specified for the loss estimates for each variety. All of this is optional, so you can use/record as much or as little of this as you like." http://veriscommunity.net/impact.html

[38] http://thinkprogress.org/justice/2015/11/11/3721521/prison-phone-hack/

[39] http://vcdb.org/

The number of data breaches is more complete than data on records lost, although those data suggest that most losses are relatively small, with several notable outliers. Nevertheless, the available data do not demonstrate that ISPs have a worse record on data security than any other industry, and it appears to be better than many.

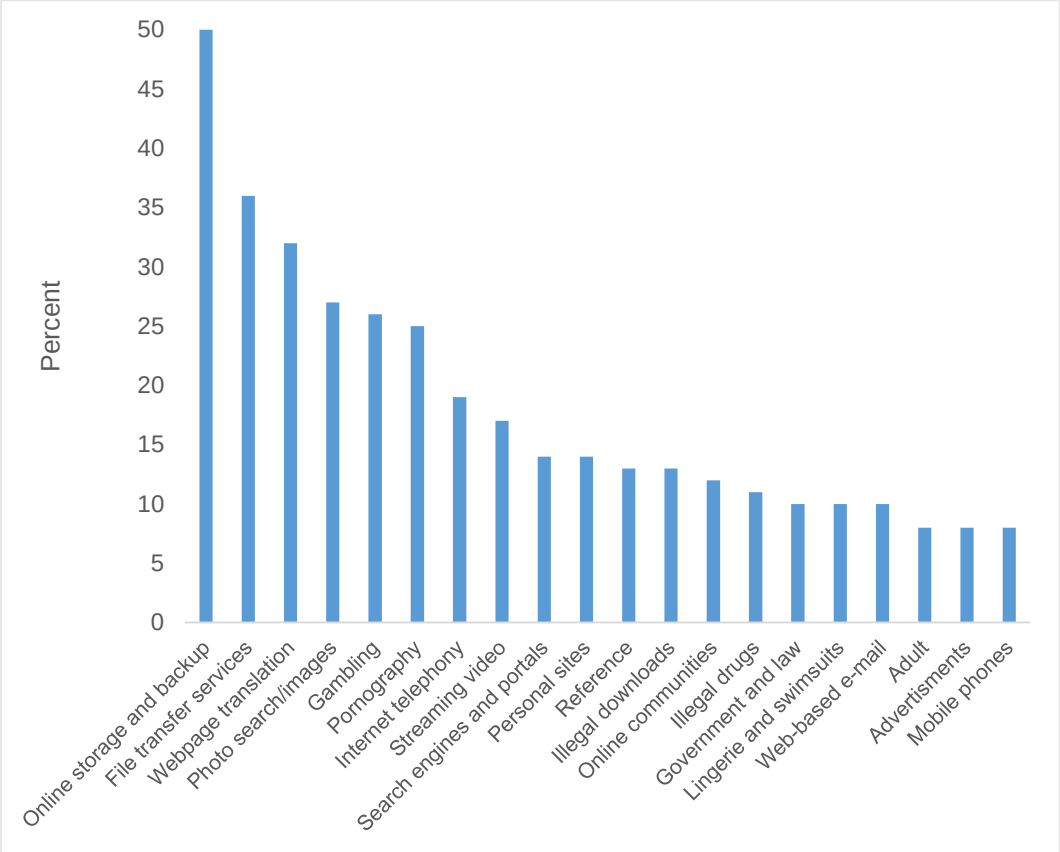
Encryption

The FCC believes that ISPs should be treated differently because, as Chairman Wheeler argued in his Senate testimony, "an ISP has a broad view of all of its customers' unencrypted online activity—when we are online, the websites we visit, and the apps we use."[40] The FCC correctly focuses on unencrypted traffic because ISPs cannot read encrypted traffic. However, as Georgia Tech professor Peter Swire, et al, note in their recent report on ISPs and privacy, "the recent and rapid shift to HTTPS and other forms of encryption is perhaps the clearest and simplest way to explain why ISPs today and in the future do not have 'comprehensive' access to users' internet activities. HTTPS blocks the possibility of ISP access to the content of users' activities – the technology called 'deep packet inspection' does not work on encrypted communications. HTTPS also blocks the possibility of ISP access to detailed URLs, which can reveal granular details of a user's search or other online activities."[41]

Encryption has been increasingly popular across the internet, especially following the Edward Snowden leak.[42] Sandvine Networks estimated that in 2015 29.1 percent of fixed internet traffic was encrypted.[43] By the beginning of 2016, that estimate had increased to 37.5 percent of fixed traffic, and 64.5 percent of mobile traffic.[44] The company estimates that by the end of 2016 "global Internet traffic will be more than 70% encrypted, with some networks surpassing the 80% threshold."[45] Figure 5 shows the dramatic rate of increase in encrypted traffic by type of traffic.

[40] Tom Wheeler, "Statement of Tom Wheeler," Presented before the Committee on the Judiciary Subcommittee on Privacy, Technology and the Law United States Senate (Federal Communications Commission, May 11, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0511/DOC-339327A1.pdf.
[41] Peter Swire, Justin Hemmings, and Alana Kirkland, "Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less than Access by Others," February 29, 2016, 9, http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.
[42] http://www.dailydot.com/politics/encryption-since-snowden-trending-up/
[43] Sandvine Intelligent Broadband Networks, "Global Internet Phenomena Spotlight: Encrypted Internet Traffic," May 8, 2015, 4.
[44] Sandvine Intelligent Broadband Networks, "2016 Global Internet Phenomena: Spotlight: Encrypted Internet Traffic," February 11, 2016, 4.
[45] Ibid., 10.

Figure 5: Encrypted Internet Traffic Increase, January-September 2015, by Category

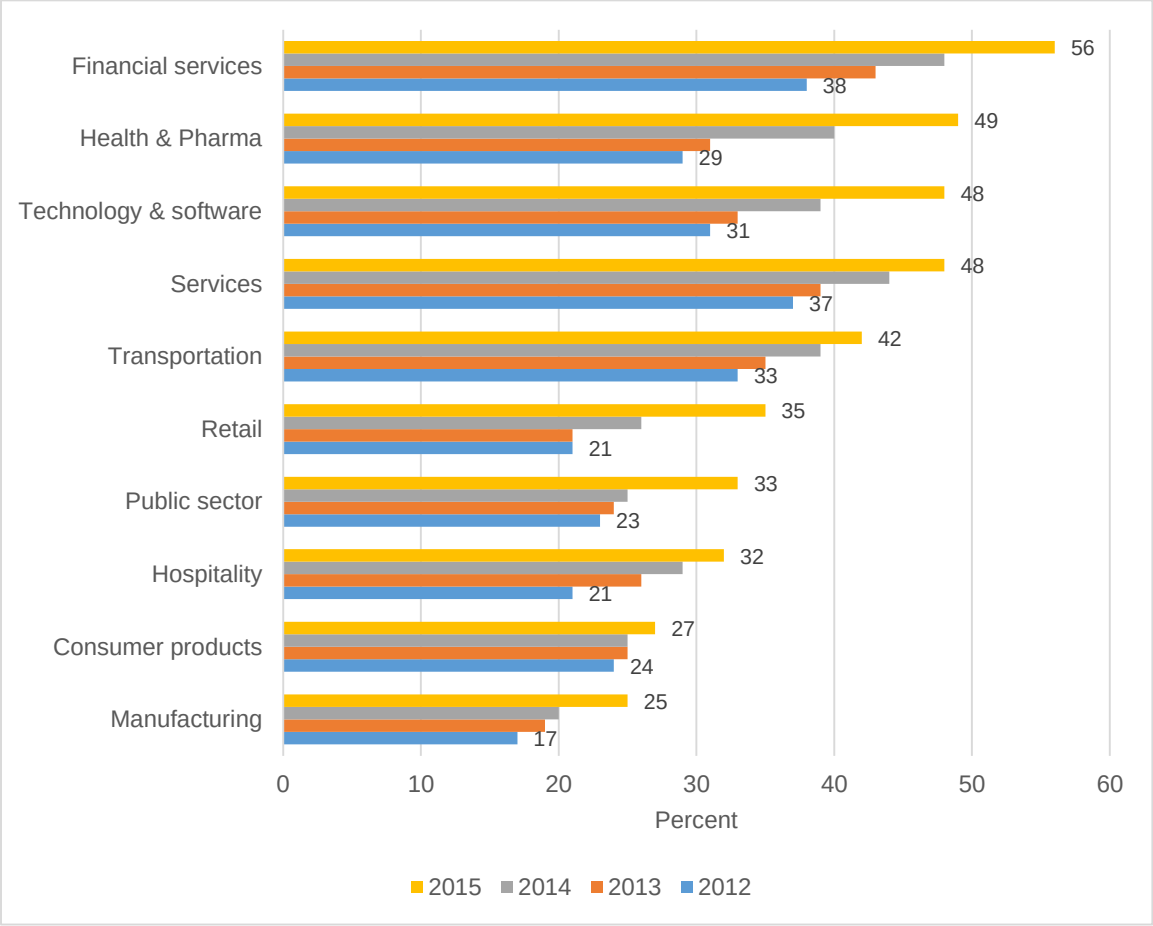


Source: Cisco Systems.[46]

According to Pew, Americans consider social security numbers and health information to be the most sensitive of their personal information.[47] Additional data shows industry responding to these concerns—companies holding that information are those adding encryption fastest (Figure 6).

[46] Cisco Systems, "Global Encrypted Internet Traffic Increase from January to September 2015, by Category," 2015, http://www.statista.com/statistics/267307/https-encrypted-traffic-increase-type-worldwide/.
[47] http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/

Figure 6: Use of Encryption by Industry, 2012-2015



Source: Ponemon 2016, Figure 7[48]

The NPRM, however, also expresses concern about encrypted traffic: "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."[49] These concerns are overstated. First, Peter Swire notes that the FCC's statement is not always true. Use of virtual private networks (VPNs) and other proxy services block an ISP's ability to see even the website the user visits.[50] Second, to the extent that an ISP could collect certain metadata about a user's online activity, the FCC does not explain why that information is necessarily more sensitive than information observed by other large platforms.

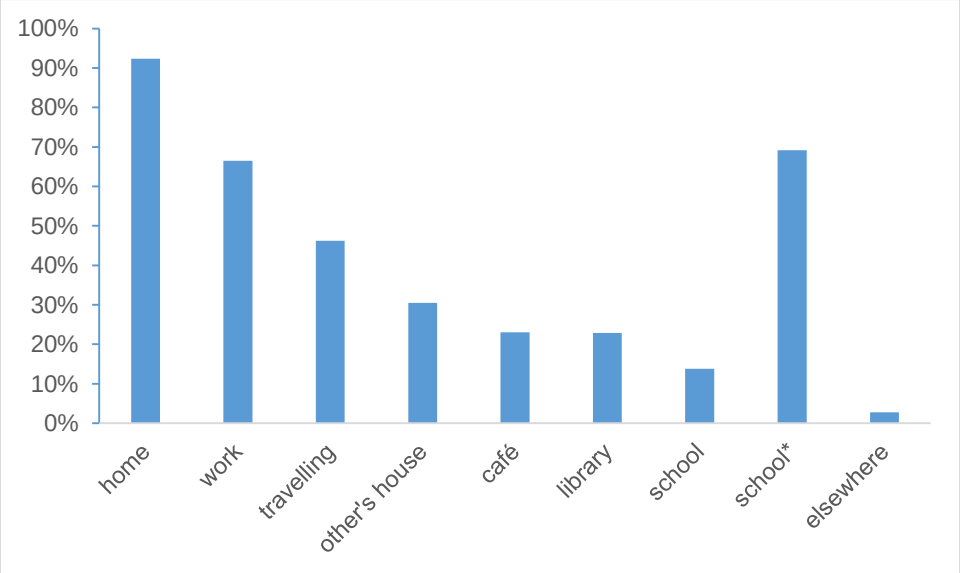
[48] Ponemon Institute, "2016 Global Encryption Trends Study," February 2016, 10.
[49] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 4.
[50] Swire, Hemmings, and Kirkland, "Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less than Access by Others."

People Access the Internet from Multiple Locations

The NPRM argues that a consumer and his ISP are joined at the hip: "because a consumer, once signed up for a broadband service, simply cannot avoid that network in the same manner as a consumer can instantaneously" switch among edge providers.[51] At first blush, this claim may sound like common sense, but as Swire et al note, "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."[52]

One factor that limits ISPs' information is that consumers do not use only a single ISP. Over the course of a day, any given user may access the internet from a home fixed connection, a mobile cellular network, various WiFi networks, and a work or school connection all the while logged in to the same email account, using the same e-commerce sites, and exploring the world with the same search engine. While we are not aware of data on the amount of time a typical consumer spends on each connection, Figure 7 shows the share of internet users over age 15 who access the internet at different locations.

Figure 7: Share of Internet Users ≥ 15 Years Old Accessing Internet at Various Places



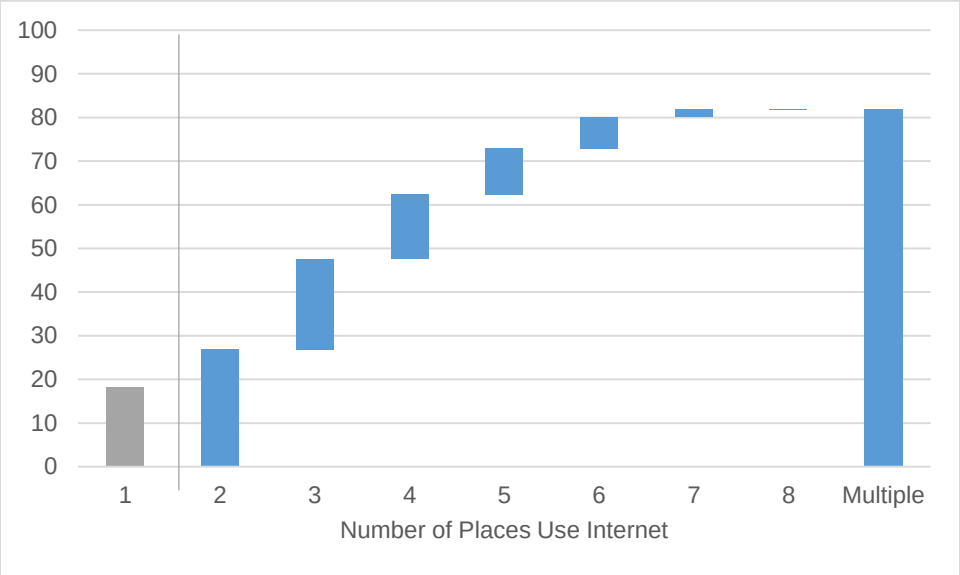
Source: Derived from U.S. Census Current Population Survey July 2015 Computer and Internet Use supplement.
*between ages 6-18

Only a small minority of internet users access the internet at only a single location. Figure 8 shows the share of internet users who access the internet at multiple locations. Less than 20

[51] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 4.
[52] Swire, Hemmings, and Kirkland, "Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less than Access by Others," 3.

percent of internet users report using the internet at only a single location,[53] more than 80 percent report using it at at least two locations, and more than half in at least three locations.

Figure 8: Share of Internet Users ≥ 15 Years Old Who Use Internet at x Locations



Source: Derived from U.S. Census Current Population Survey July 2015 computer and internet supplement.[54]

A rejoinder to that observation may be that even if they log on in many places throughout the day, consumers cannot "instantaneously" move from one ISP to another as they can with edge platforms, as the FCC contends. But that is not generally true either literally or in the spirit of why a consumer would want to switch "instantaneously."[55] A person using a search engine can switch from Google to, say, DuckDuckGo, for searches he would rather not share with Google. Similarly, people with a smartphone and a fixed connection could switch from one to the other or a VPN if they do not want a particular ISP to know the terminating site.

The NPRM suggests that ISPs "have the commercial motivation to use and share extensive and personal information about their customers,"[56] but does not acknowledge a countervailing incentive to protect their customers' privacy. ISPs compete to attract customers from each other, and even if prospective customers do not choose an ISP based on privacy concerns, no company wants the financial costs and negative attention that accompany a privacy breach.

[53] More specifically, 18.1 percent of internet users (not of the general population) report using it in a single location. Breaking that down further, 13.2 percent of internet users access the internet only from home, 3.2 percent from work, and the remainder from the other places listed in Figure 4.
[54] Share is of respondents at least 15 years old who reported using the internet anywhere and answered all questions about where they use it.
[55] Wallsten suggests that the laws of physics, rather than switching costs, prevent humans from making any such change instantaneously, but agrees they may be able to change instantly.
[56] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 3.

The above discussion shows, more generally, that there is no basis for saying that either ISPs or edge companies necessarily have more information about users or more insight into their lives than the does the other. Applying stricter privacy rules to one over the other is arbitrary.

Link Between Privacy Concerns and Broadband Adoption is Weak, at Best

The NPRM argues that strong privacy rules are likely to stimulate broadband investment and adoption. The FCC's argument has two problems. First, if its argument is true, it should apply also to edge companies, and is thus unrelated to the claim that ISPs deserve special attention, especially given the lack of evidence that consumers worry more about privacy with respect to their ISP than with respect to edge companies. Second, the NPRM vastly overstates the case for a connection between privacy concerns and network buildout and adoption.

To support its argument, the NPRM appeals to past FCC documents, claiming that "we have previously found that protection of privacy encourages broadband usage that, in turn, encourages investment in broadband networks."[57] But the Commission has not, in fact, made any such finding. The NPRM cites paragraph 464 of the Open Internet Order, which says

> We find that if consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand. As the Commission has found previously, the protection of customers' personal information may spur consumer demand for those services, in turn "driving demand for broadband connections, and consequently encouraging more broadband investment and deployment" consistent with the goals of the 1996 Act.[58]

The Open Internet Order, in turn, cites paragraph 104 of the FCC's 2015 Broadband Progress Report. That paragraph says "we note that there are indications that there is a correlation between [privacy] concerns and non-adoption of broadband…."[59] The Progress Report suggests only "indications of a correlation" because that is an accurate portrayal of the evidence it cites. In particular, that paragraph cites a 2009 survey that found "Non-adopters are almost 50 percent more likely than broadband users to say they believe it is too easy for personal information to be stolen online."[60] That same survey, however, did not find privacy concerns to be a primary reason for non-adoption. Instead, the top three reasons for non-adoption at the time were "cost" (36 percent of non-adopters), digital literacy (22 percent), and relevance (19 percent).[61]

Other surveys confirm there is little connection between privacy concerns and adoption. The same FCC Broadband Progress report quotes from an NTIA report, which said "only 1 percent of

---

[57] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 11.
[58] Federal Communications Commission, "In the Matter of Protecting and Promoting the Open Internet," Report and Order on Remand, Declaratory Ruling, and Order, (February 6, 2015), para. 464, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.
[59] Federal Communications Commission, "2015 Broadband Progress Report," January 29, 2015, para. 104, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-10A1.pdf.
[60] John B. Horrigan, "Broadband Adoption and Use in America," OBI Working Paper (Federal Communications Commission, October 2010), 4, https://apps.fcc.gov/edocs_public/attachmatch/DOC-296442A1.pdf.
[61] Ibid., 5.

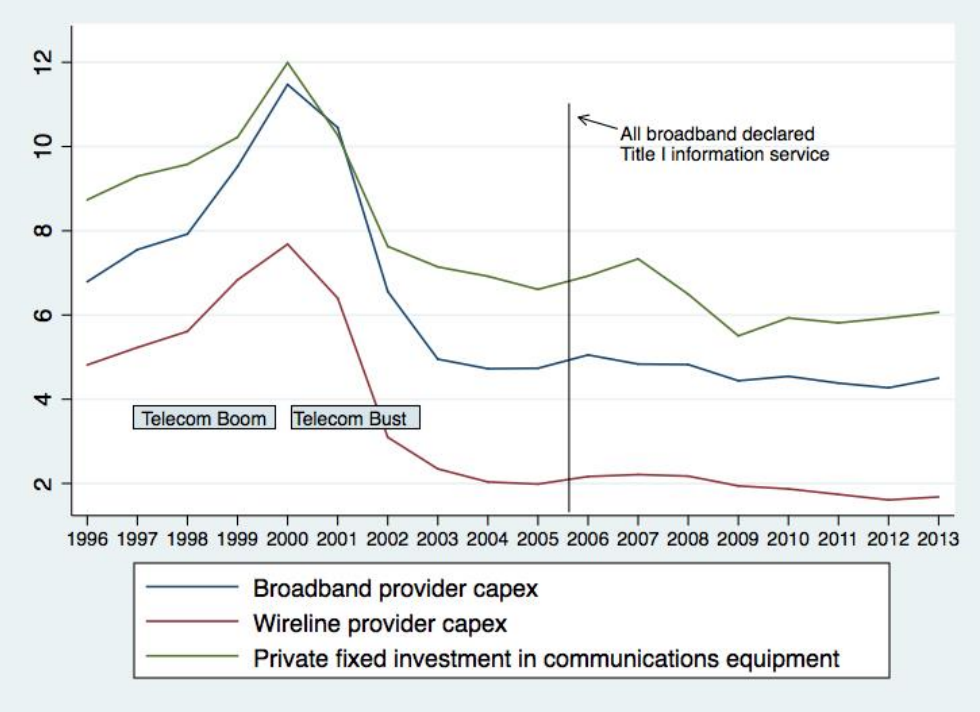
households expressed privacy concerns in both 2011 and 2012 as their primary reason for not using the internet at home…."[62] That same sentence continues by expressing the concern that despite the low share of people who claim not to use the internet at home, "well-publicized data breaches and greater consumer awareness of internet privacy issues may affect this response in future years."[63] As it turned out, however, "data breaches and greater consumer awareness of internet privacy issues" did not affect this response: The July 2015 Computer and Internet Use Supplement to the Current Population Survey finds that less than one-half of one percent of non-adopters note privacy concerns as the key reason they do not use the internet.[64] Similarly, in a 2015 Pew survey, less than one percent of respondents who do not own smartphones cite privacy concerns as a reason.[65]

The FCC also contends that strong privacy protection generates investment in broadband networks.[66] In particular, the Commission argues that "[t]he largest investment ever in wireline networks came during those years in which DSL Internet access services were regulated under Title II."[67] Regardless of the truth of the assertion regarding investment, this argument is weak. The FCC provides no evidence that rules regarding privacy were at all related to investment.

Moreover, the claim that those years saw "largest investment ever in wireline networks" is misleading, at best. The period of time the Commission cites includes the dot-com boom and bust. If the Commission wants to attribute the boom to Title II then, presumably, it also attributes the bust to Title II (Figure 9).

[62] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 464.
[63] Ibid.
[64] Analysis of July 2015 Current Population Survey Computer and Internet Use Supplement.
[65] John B. Horrigan and Maeve Duggan, "Home Broadband 2015: The Share of Americans with Broadband at Home Has Plateaued, and More Rely Only on Their Smartphones for Online Access" (Pew Internet and American Life Project, December 21, 2015), http://www.pewinternet.org/2015/12/21/home-broadband-2015/.
[66] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 11.
[67] Ibid.

Figure 9: Telecom Boom and Bust Concurrent with Title II Investment as Share of GDP (x1000)

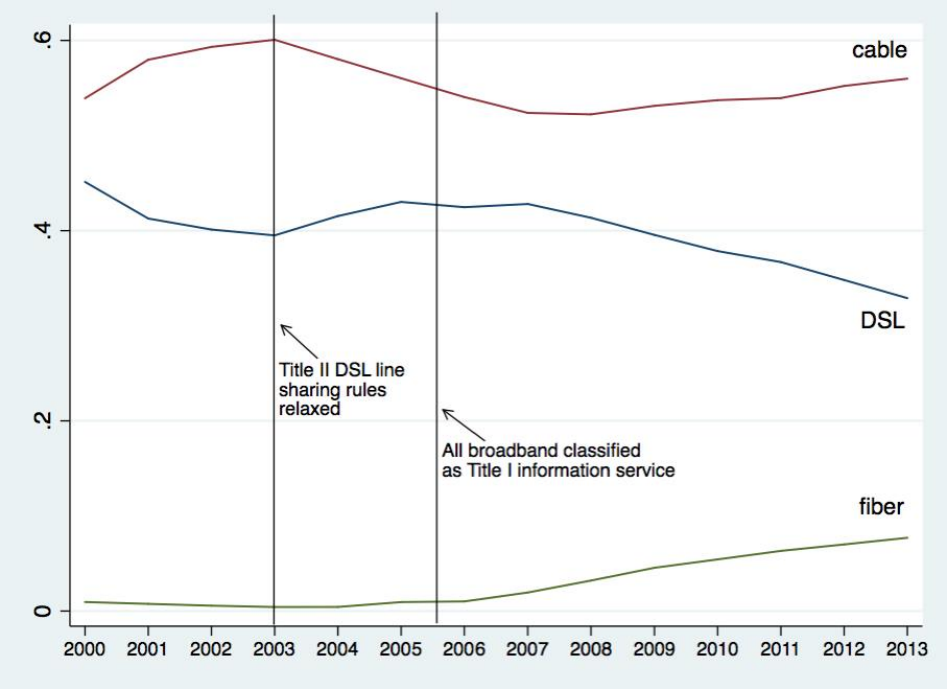


Sources: USTelecom, U.S. Bureau of Economic Analysis[68]

Additionally, the evidence suggests that Title II, overall, was not good for investment. While DSL was regulated under Title II and cable was not, cable broadband dominated DSL. Once DSL's line sharing requirements were loosened the trend reversed, and once all broadband was declared an information service regulated under Title I, the traditional telephone companies began investing in fiber (Figure 10).

[68] Broadband provider capex: US Telecom https://www.ustelecom.org/sites/default/files/images/Historical-Broadband-Provider-Capex-072015-big.png (last accessed May 16, 2016); Wireline provider capex: US Telecom and 451 Research (last accessed via Statista May 16, 2016); Private fixed investment in telecommunications equipment: U.S. Bureau of Economic Analysis, http://www.bea.gov/histdata/Releases/GDP_and_PI/2014/Q1/Second_May-29-2014/UND/Section5ALL_xls.xls, Table 5.5.5U series C275RC0.

Figure 10: Share of Fixed Broadband Connections by Technology



Sources: FCC Internet Access Services Reports

Regardless of one's views on the effects of Title II, to our knowledge no empirical study has attempted to separate the effects of privacy rules that previously existed under Title II regulation from any other aspect of Title II.

While people are concerned about privacy, evidence shows those concerns have not prevented them from increasingly conducting transactions online. Data from the July 2015 CPS Computer and Internet Use supplement show more people engaging in financial transactions and online shopping in 2015 than in any previous year (Figure 11).

Figure 11: Share of Internet Users Reporting Engaging in Online Transactions, 2011-2015

Source: U.S. Census Current Population Survey Computer and Internet Use Supplement, July 2015

Few would argue that privacy concerns are not important, and it is possible that internet adoption and use would be even more robust were internet users less concerned about privacy. However, the NPRM does not cite evidence showing that to be the case. The available data seem to show the contrary.

The FCC's Privacy Proposal is Stricter than Previous Privacy Rules

The FCC asserts that the proposal would "implement the core principles of transparency, choice, and security by proposing regulations to ensure that consumers (i) have the information needed to understand what data the BIAS provider is collecting and what it does with that information, (ii) can decide how their information is used, and (iii) are protected against the unauthorized disclosure of their information."[69] The proposal, however, is based on an outdated approach to privacy and relies heavily on consumer "opt-in," which would almost certainly eliminate the many benefits that come from use of data.

Much of FIPPs is Outdated

The Commission bases its proposal on the Fair Information Practices Principles (FIPPs).[70] These principles date back to the 1970s and have been the focus of privacy discussions since then. The FIPPs are reflected in the OECD Privacy Principles of 1980, current European Union regulations, and the recommendations of the FTC's 2012 Privacy Report.[71]

---

[69] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 14.
[70] Ibid., para. 5.
[71] For an excellent summary of the evolution of the FIPPS, see Robert Gellman, "Fair Information Practices: A Basic History," December 4, 2015, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

The FIPPs, however, with their focus on limiting data collection and use, are now increasingly irrelevant and costly, as two recent White House reports on big data acknowledge.[72]

Principles of notice and choice regarding how data are used and collected, which are principal elements of the FIPPs, become almost meaningless when data may be used in unpredictable ways. The White House report, for example, observes that new sources of data and types of data analysis "may require us to look closely at the notice and consent framework that has been a central pillar of how privacy practices have been organized for more than four decades."[73] Moreover, as the PCAST report notes, "As a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data. It is simply too complicated for the individual to make fine-grained choices for every new situation or app."[74] Moreover, "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[75]

The NPRM, which requires that data should only be collected for a specific, identified purpose, ignores these well-understood principles of data. Unanticipated uses and sharing arrangements would presumably require additional opt-in consent from all individuals represented in a data set. Limiting the reuse or sharing of data precludes the innovative ways in which big data are being used in a variety of sectors, from marketing to credit markets to health research.

The NPRM also highlights the transparency element of the FIPPs framework.[76] The notion that consumers should understand who is collecting their data and how the data are being used seems appealing at first blush, but in the big data era where hundreds of data points and complex calculations are used to create some kind of score or index and may change rapidly, it is likely to be impractical and not especially meaningful to consumers. That is, this information cannot be meaningfully conveyed through a simple notice, and consumers would not devote the hours required to understand it. For example, it is not clear that a person rejected for credit by a complex algorithm would particularly benefit by being shown the equation used. How a ratings agency arrives at a consumers' FICO score, an early example of a calculation based on a complex algorithm, is virtually impossible to explain to even an informed consumer because of interactions and nonlinearities in the way various data points enter into the score.[77]

As an alternative to the standard FIPPs approach, the White House Report suggests examining "whether a greater focus on how data is used and reused would be a more productive basis for managing privacy rights in a big data environment."[78] The PCAST Report is even clearer:

---

[72] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values"; President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective."
[73] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values," 54.
[74] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective," 38.
[75] Ibid., xi.
[76] The White House, Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy and Promoting Innovation in the Global Digital Economy, February, 2012 pg. 14-15
[77] The major inputs to a credit score are well known; however, the calculation of credit scores from credit report data is proprietary and exceedingly complex. See for example FDIC, *Credit Card Activities Manual*, Ch. 8 – Scoring and Modeling, 2007, available at: http://www.fdic.gov/regulations/examinations/credit_card/.
[78] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values," 61.

> Policy attention should focus more on the actual uses of big data and less on its collection and analysis. By actual uses, we mean the specific events where something happens that can cause an adverse consequence or harm to an individual or class of individuals…. By contrast, PCAST judges that policies focused on the regulation of data collection, storage, retention, a priori limitations on applications, and analysis… are unlikely to yield effective strategies for improving privacy. Such policies would be unlikely to be scalable over time, or to be enforceable by other than severe and economically damaging measures.[79]

The FCC should follow the White House's lead and carefully think through the economic implications of imposing 1970s-era privacy rules today.

Opt-In or Opt-Out

Whether the default for consumer data collection should be "opt-in" or "opt-out" has been under discussion virtually since the beginning of the commercial internet.[80] That is, if consumers make no decision, who has the right to control the use of information? Under opt-in, the consumer by default controls information use and the website must obtain permission from the consumer to use information. Under opt-out, the website has the default right to use information about the consumer, and the consumer must make an effort to change this by opting out.

The NPRM divides customer information into three categories:[81]

- Customer data necessary to provide the broadband service, for which no approval is necessary.
- Data used to market communications-related services, for which opt-out approval is required.
- All other data, for which opt-in approval is needed.

Edge providers, in general, are not required to have users opt-in to collect their data. Such approval is normally required only for sensitive information, such as health or financial information. In contrast, the FCC has chosen to require opt-in approval for almost all data that might be collected and used for commercial purposes by ISPs, most of which is non-sensitive. Under these rules, ISPs would operate under uniquely stringent requirements as compared to other sectors of the economy and the rest of the online world.

Richard Thaler and Cass Sunstein discuss the importance of the choice of default in their popular book *Nudge*.[82] They argue that "humans will often consider required choice to be a nuisance or worse, and would much prefer to have a good default… When choice is complicated and difficult, people might greatly appreciate a sensible default."[83] They cite a study of opt-in versus opt-out enrollment in 401(k) plans, for which initial participation for opt-in plans was only 20

---

[79] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective," xiii.
[80] Although that debate had died down in recent years until the FCC's proposal.
[81] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 18.
[82] Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness*, New internat. ed (London: Penguin, 2009).
[83] Ibid., 86–87.

percent, eventually rising to 65 percent over three years, compared to 90 percent and 98 percent for an opt-out plan. They conclude that "automatic enrollment thus has two effects: participants join sooner, and more participants join eventually."[84] Therefore, setting the default choice has an appreciable impact on the eventual number of participants in a program.

The key insight here, as in many other situations, is that transactions costs matter. If transaction costs are zero, then the choice of the default—for our purposes, the initial allocation of the right to control the use of information—does not matter. If, however, transactions costs are positive, it is efficient to give the right to the party who values it the most, or the party who would buy it if transaction costs were zero.[85]

We observe that most consumers are willing to trade information for something useful to them. As discussed above, the purpose of obtaining information about consumers is to provide them with targeted advertising—advertising of products likely to be of use to them—as well as with services, such as free search and email. Given that consumers want to engage in those transactions, if transactions costs were zero, websites would end up with the information because consumers would opt to provide their information whether that required opting in or not opting out. Because transactions costs are not zero, efficiency argues for giving the initial right to businesses—that is, for opt-out. If the default is opt-in, then information is lost—it does not flow to its highest-valued uses.[86] This loss of information is costly and leads either to price increases as firms attempt to compensate for the loss of information or elimination of services.

It might appear that the transaction costs associated with making a decision about data collection are low, and therefore the default would not matter. However, Thaler and Sunstein show that the costs are sufficiently high that consumers have a tendency to not change the default, whatever it might be. One consultant indicated in testimony to the FTC that with opt-out, one firm would lose about 5 percent of participants, while with opt-in they would lose about 85 percent.[87] The tendency of consumers to not change the default could arise from transactions costs of learning about the nature of the choice are high or because the consumers do not care enough about the issue to invest any time in making the choice.

Sovern, who argued in favor of a mandatory opt-in system, provided an example that indicates the sort of transactions costs associated with opt-in:

> Evidence on how companies behave in an opt-in environment suggests that such a system may be more efficient for consumers than the current system. After the FCC ruled that phone companies seeking to use phone-calling patterns for marketing purposes must first obtain the consumer's permission, the telephone company in my area attempted to secure that permission. Its representatives called and sent mailings to subscribers. The company also set up a toll-free number for consumers with questions. The mailing I received was brief, printed in different colors, and written in plain English. It also promised, in words which were underlined, that

[84] Ibid., 109.
[85] See, for example, Richard A. Posner, *Economic Analysis of Law*, 7th ed (New York, NY: Wolters Kluwer Law & Business : Aspen Publishers, 2007).
[86] Eli Noam, "Privacy and Self-Regulation: Markets for Electronic Privacy," Privacy and Self-Regulation in the Information Age vols. (U.S. Department of Commerce, 1997); Hal R. Varian, "Economic Aspects of Personal Privacy," in *Privacy and Self-Regulation in the Information Age* (U.S. Department of Commerce, 1997).
[87] Testimony by Larry Ponemon, PriceWaterhouseCoopers, at the FTC hearing, *Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, December 12, 2000, Vol. 2, p. 232.

> "we'll never share this information with any outside company." A postage-paid envelope and a printed form were included for consumers to respond. Consumers who accept the offer need only check a box, sign and date the form, and print their name. The company also offered consumers incentives to sign up—such as a five-dollar check, two free movie tickets, or a ten-dollar certificate from certain retailers—thus increasing the likelihood that consumers will pay attention to the information. In sum, the company has done everything it can to eliminate consumer transaction costs.[88]

Although this procedure may have reduced consumer transactions costs, it increased total transactions costs substantially. The increased transactions costs incurred by businesses trying to induce consumers to opt-in are also a nuisance for consumers.[89] US West (using telemarketing) obtained an opt-in rate of 29 percent among residential subscribers at a cost of $20.66 per positive response.[90] These higher transactions costs are ultimately paid by consumers, either through higher prices or reduced services and benefits.

Under the FCC's proposal information could be used only for the purpose for which it was collected, unless consumers provided additional opt-in consent. Such a restriction on information use would preclude many productive uses, including security-related uses. In other words, the proposal would eliminate the option value of data, reducing the benefits its use can generate.

Finally, as explained in a recent paper by Campbell, Goldfarb and Tucker, the transactions costs to consumers associated with notice and choice privacy regulation can also have an anticompetitive effect.[91] These transactions costs would be larger in an opt-in world. Notice and choice regimes typically require obtaining consent one time (or at least consent requests don't increase proportionately with amount of data). Therefore, as with the fixed costs of privacy regulations faced by firms, the user transactions costs associated with notice and choice requirements disproportionately affect smaller firms. Campbell, Goldfarb and Tucker conclude that "the nature of transactions costs implied by privacy regulation suggests that privacy regulation may be anticompetitive,"[92] and that "a potential risk in privacy regulation is the entrenchment of the existing incumbent firms and a consequent reduction in the incentives to invest in quality."[93]

Similar reasoning suggests that the transactions costs associated with notice and choice, and particularly with an opt-in regime, would be an impediment to switching ISPs. This is because a consumer who wants to sign up for a new ISP will have to incur these costs an additional time. The NPRM cites switching costs as a major reason for singling out ISPs for special treatment. Those switching costs would rise if the proposed rules to into effect.

---

[88] Jeff Sovern, "Opting In, Opting Out, Or No Options At All: The Fight for Control of Personal Information," *Washington Law Review* 74 (October 1999).
[89] Discussed in Fred H. Cate and Michael E. Staten, "Protecting Privacy in the New Millennium: The Fallacy of 'Opt-In'," Information Services Executive Council, available at http://www.the-dma.org/isec/optin/shtml.
[90] As cited in Michael A. Turner, "The Impact of Data Restrictions on Consumer Distance Shopping" (The Direct Marketing Association, 2001).
[91] James Campbell, Avi Goldfarb and Catherine Tucker, Privacy Regulation and Market Structure, Journal of Economics and Management Strategy, vol. 24, no. 1, Spring 2015, 47-73.
[92] Ibid, 48.
[93] Ibid, 68.

Data Breach Notification

The NPRM states that the proposed data breach notification requirements "seek to incorporate the lessons learned from existing and proposed data breach notification frameworks…"[94] However, the NPRM leaves to the imagination the lessons it has incorporated and why, as it provides no explanation as to how past experiences informed its proposal.

The NPRM asks whether reporting or notification requirements should be based on the likelihood of harm to consumers.[95] It seems generally established that notification requirements should be grounded in the risks presented by the breach. As the European Network and Information Security Agency noted:

> Notifications should follow breaches of personal data that are likely to cause harm to data subjects or violate their rights. For example, if breached data is encrypted, there may be no real risk that the data will be exploited, and consequently a notification would be redundant. Issuing notifications for breaches that pose no risk will undermine customers' confidence in the organisation, and cause fatigue for data subjects, data controllers and regulatory authorities. Issuing notifications in cases where there is no risk could also desensitise customers and, as a result, they may overlook more serious notifications. It would be useful to provide guidance or develop guidelines for determining risk for both data controllers and regulatory authorities.[96]

The FCC acknowledges this concern: "Recognizing the harms inherent in overnotification (or 'notice fatigue'), the NPRM proposes to adopt a trigger as to when notice is needed, and seeks comment on under what circumstances BIAS providers should be required to notify customers of a breach of their PI."[97]

While "recognizing the harms…," the FCC proposes adopting a hair-trigger response to almost any breach whatsoever. The proposal would require ISPs to notify customers of any data breach within 10 days.[98] The FTC, by contrast, allows for different types of responses depending on the severity of the breach in terms of the number of people affected and type of information revealed. For breach of health records, for example, the FTC requires firms to notify the FTC within 10 days if the breach involves more than 500 people but has 60 days to notify consumers.[99] Indeed, in 2011 the Obama administration proposed establishing a 60-day notification period.[100]

A 10-day notification period for any breach regardless of severity seems to risk creating the "notification fatigue" that concerns the FCC. Moreover, it may not give the relevant entities

---

[94] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 233.
[95] Ibid., paras. 237–238.
[96] European Network and Information Security Agency, "Data Breach Notifications in the EU," 2010, 33.
[97] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 23.
[98] Ibid.
[99] https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule
[100] The White House, "Data Breach Notification Legislative Language," May 2011, 3, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf.

enough time to understand the nature of the breach. The FTC notes, "[t]he purpose for the 60 day period is to give entities time to conduct…an investigation."[101]

Determining the level of risk is not always simple. As Sandvine Networks has noted,

> As the criteria for determining a breach can be broad, there is a chance that even frivolous breaches that pose no real risk to the rights of data subjects could require notifications. In order for procedures to be effective, there is a view that decisions should be risk-based. In other words, if there is no real risk to the data subjects, a notification would be redundant. For example, if the data breached was encrypted, it is not likely that the information could be exploited in any way. Consequently, regulatory authorities and data controllers alike are faced with the challenge of determining the level of risk that each breach poses, so as to avoid disproportionate responses to potentially frivolous breaches. In most cases, regulatory authorities did not have any formal criteria for measuring risk. Consequently, determining risk is done mostly on an ad hoc basis.[102]

The NPRM displays the type of ad hoc approach described in the Sandvine report. The proposal provides no explanation for why the FTC's 60-day notification period for breaches of some of the most sensitive personal data is insufficient for breaches of any data an ISP may have. Indeed, the NPRM includes no discussion of the experience under existing frameworks or of data breaches experienced by ISPs.

A reasonable first step before issuing rules would be for the Commission to first analyze the costs of security breaches experienced by ISPs. Those costs consist primarily of credit card fraud, although some victims of data breaches experience more severe types of identity theft. The benefits of data breach notification requirements will consist of a reduction in those costs. Even when consumers are notified, however, many do nothing about it. For most people, this is probably a rational response, because only a small percentage of consumers whose records are compromised actually experience some sort of identity fraud and "doing something about it" is not costless.

The costs of notification include the direct notification costs; the costs of actions taken by consumers as a result of notification; and the costs in terms of diminished flow of information. Costs to consumers from actions they might take include placing fraud alerts on accounts or even closing accounts. A fraud alert means that businesses must verify the consumer's identity before issuing credit, which might cause delays in obtaining credit. Closing accounts can be particularly costly for consumers who have set up accounts to pay recurring bills automatically. These costs may be greater than the expected costs (to the consumer) of actually being victimized by credit card fraud.

If consumers start seeing numerous notices, they may start to ignore the notices or, alternatively, become afraid of doing business online. This may in some cases, increase the likelihood of fraud, much of which occurs offline. It also would be inconsistent with the Commission's goal for its regulations to promote broadband use. Alternatively, requiring firms to react in a

[101] https://www.gpo.gov/fdsys/pkg/FR-2009-08-25/pdf/E9-20142.pdf p.42971
[102] European Network and Information Security Agency, "Data Breach Notifications in the EU," 17.

particular way regardless of the severity of the breach, they may choose not to pursue productive uses of their data or productive sharing arrangements with other firms.

Competition, Competition, Competition: The Effects of the FCC's Privacy Proposal

In addition to the overall problems of failing to take into account the benefits of information and evaluating whether the previously-existing FTC approach to privacy and security is inappropriate, the rules may have real effects on advertising markets and, in particular, digital marketing. These effects matter for several reasons. First, the market for advertising is large, meaning it matters even without considering its effects on ISPs.

If ISPs are subject to the FCC's proposed rule, with its opt-in requirement and stricter breach notification requirements, they will be at a competitive disadvantage to edge companies and it will be more difficult for ISPs to become significant players in the digital advertising market. The second reason the effect matters, therefore, is that the online advertising market may be less competitive than it otherwise would be and costs for online advertising will be higher.

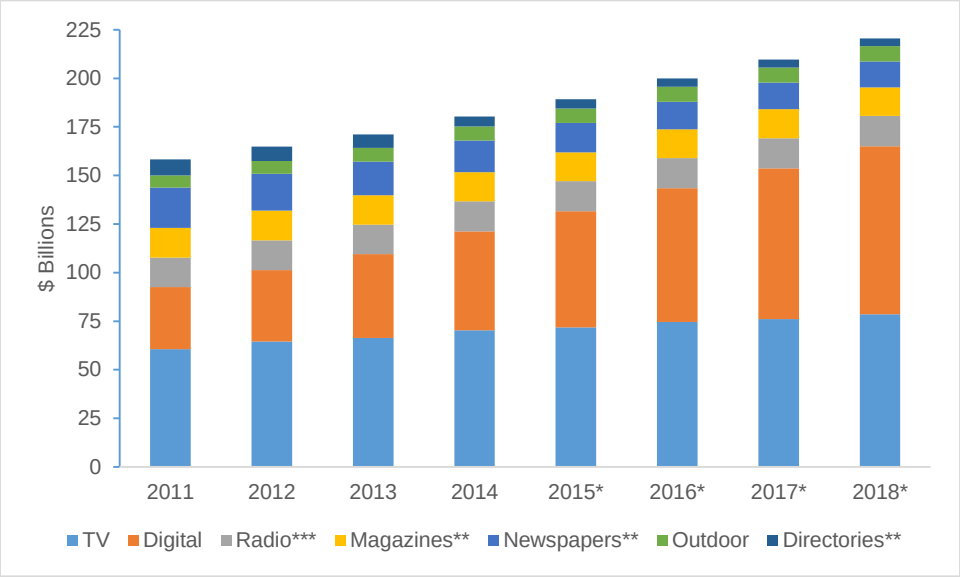
Finally, the rules may foreclose a revenue source for ISPs in the future, ensuring that consumers continue to bear the brunt directly of costs and making entry for new ISPs more difficult.

The Advertising Market is Large

The advertising market is large and the digital component of it is growing. Spending on media advertising is expected to be around $200 billion in 2016, with digital advertising in particular projected to grow from about $32 billion in 2011 to $86 billion in 2018 (Figure 12). By contrast, PwC estimates that revenues from fixed broadband access will be $56 billion in 2016.[103]

[103] PwC. *Fixed broadband access revenues in the United States from 2011 to 2017 (in million U.S. dollars).* http://www.statista.com/statistics/280435/fixed-broadband-access-revenues-in-the-united-states/ (accessed May 20, 2016).

Figure 12: Media Advertising Expenditures by Media Type



* projected; ** print only; *** excludes off-air radio and digital
Source: Derived from eMarketer[104]

The White House Office of Information and Regulatory Analysis (OIRA) requires executive agencies to perform a cost-benefit analysis on any proposed rule that will "have an annual effect on the economy of $100 million or more…"[105] Independent agencies are not subject to OIRA rules, but the threshold is useful for analyzing whether the FCC should concern itself with the question. $100 million is only 1.5 percent of digital advertising expenditures—even less in the future as digital advertising grows or if the effects spill over into the non-digital side of the advertising market. In other words, even a small relative expected effect of the rule on the advertising market would be enough to require an executive branch agency to conduct a cost-benefit analysis. That, alone, should be enough for the FCC to at least take the effects on advertising seriously even before considering the effects on ISPs and advertisers.

The Rules May Reduce Competition in Advertising Markets

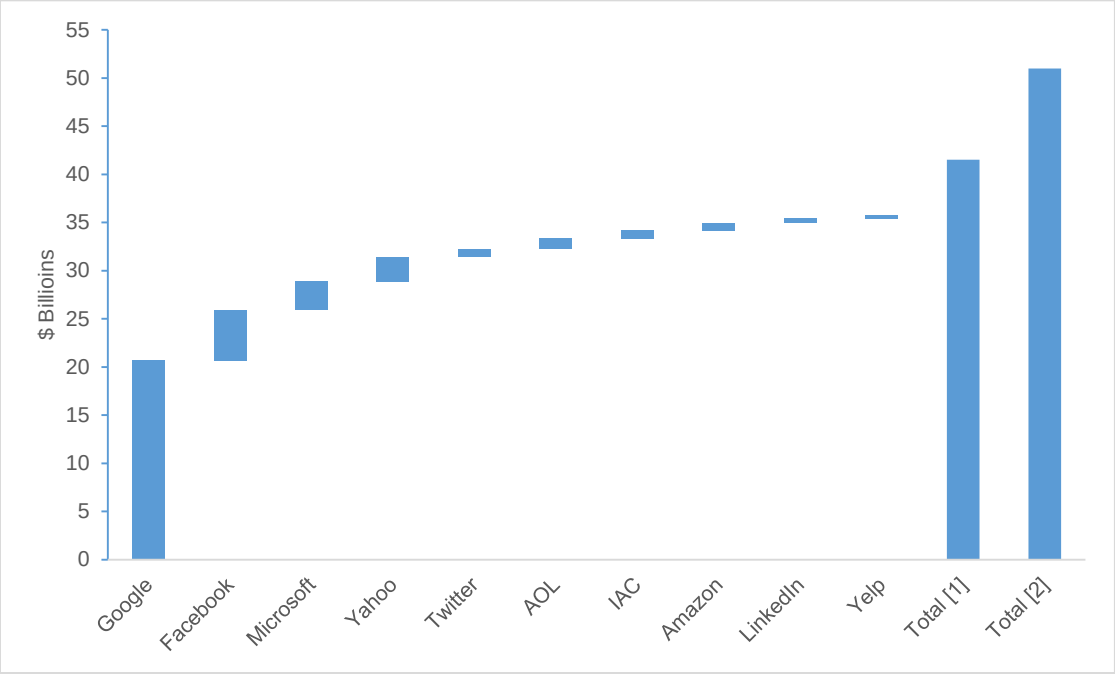
The asymmetric nature of the rules may have competitive effects. In particular, the FCC's proposal would reduce competition and potential competition in the growing market for digital advertising, potentially harming the businesses that rely on advertising to reach consumers for their products. Thus far, the market for digital advertising has been dominated by edge companies, such as Google, Facebook, and others who operate under the FTC's privacy enforcement regime (Figure 13). ISPs are not currently a major presence in digital marketing.

---

[104] Total spending amount: eMarketer. Media advertising spending in the United States from 2011 to 2018 (in billion U.S. dollars). http://www.statista.com/statistics/272314/advertising-spending-in-the-us/ (accessed May 20, 2016); Share by media type: eMarketer. *Distribution of advertising spending in the United States from 2010 to 2019, by media*. http://www.statista.com/statistics/272316/advertising-spending-share-in-the-us-by-media/ (accessed May 20, 2016).

[105] https://www.whitehouse.gov/omb/OIRA_QsandAs

Figure 13: U.S. Net Digital Advertising Revenues by Firm, 2014

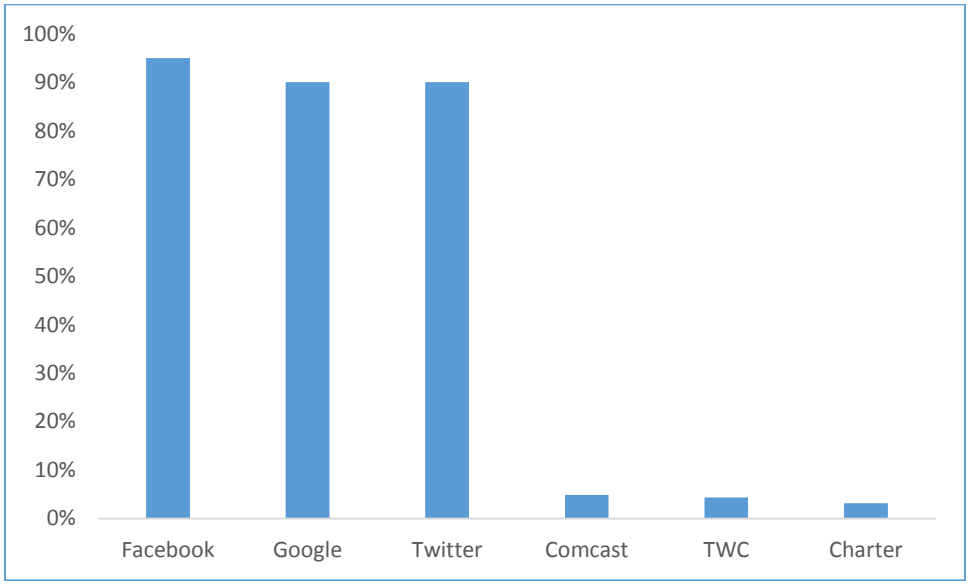


Notes and Sources: Estimates of total digital advertising differ by source. Total[1] is from Dentsu Aegis Network;[106] Total [2] is from eMarketer;[107] Revenues by firm are from eMarketer.[108]

ISPs do not disclose their digital advertising revenues. However, we can infer from their total advertising revenues that it is small. Some edge providers, like Google and Facebook, rely almost entirely on advertising for their revenues. ISPs have typically operated under a different model: consumers pay them directly for the services they receive. Figure 14 shows advertising as a share of revenue for the largest ISPs and edge providers. The figure reflects total advertising revenues; the share of revenues from digital advertising for the ISPs is therefore even smaller.

[106] Dentsu Aegis Network. *Digital advertising expenditure in the United States from 2008 to 2015 (in million U.S. dollars)*. http://www.statista.com/statistics/386984/digital-advertising-expenditures-usa/ (accessed May 20, 2016).
[107] eMarketer. *Media advertising spending in the United States from 2011 to 2018 (in billion U.S. dollars)*. http://www.statista.com/statistics/272314/advertising-spending-in-the-us/ (accessed May 20, 2016).
[108] eMarketer. *Net digital advertising revenue of selected online companies in the United States from 2014 to 2017 (in billion U.S. dollars)*. http://www.statista.com/statistics/460687/digital-ad-revenue-select-companies/ (accessed May 20, 2016).

Figure 14: Advertising as Share of Revenues, 2015



Sources: 2015 Company SEC 10K filings

We do not know what the optimal market structure looks like for digital marketing. It is possible that the market will not support significant entry. After all, by all indications Google and Facebook, and to a lesser extent, Twitter, are fighting fiercely via innovation for advertising dollars.[109] Nevertheless, just as the FCC would (and should) be loath to discourage entry into the ISP market regardless of its views on the state of competition, it should similarly avoid increasing the cost of entry into digital advertising.

Even if ISPs do not gain significant traction in digital marketing, the threat of entry can significantly affect the market. Google Fiber, for example, passes a relatively miniscule number of households—only about 400,000 by mid-2015 by one estimate and confirmed expansion to about 2.4 million homes within a few years.[110] But Google continues to announce new buildout plans, and incumbent ISPs have responded to this threat.[111]

[109] See, for example, Erin Griffith, "How Google Is Attacking Facebook's Mobile Advertising Stronghold," *Fortune*, April 21, 2016, http://fortune.com/2016/04/21/google-facebook-mobile-advertising/; Chris Ciaccia, "Facebook and Google Are Sucking Up Ad Dollars From Everyone Else -- Here's One Simple Reason Why," *TheStreet*, January 23, 2016, https://www.thestreet.com/story/13432686/1/facebook-and-google-are-sucking-up-ad-dollars-from-everyone-else-here-s-one-simple-reason-why.html.

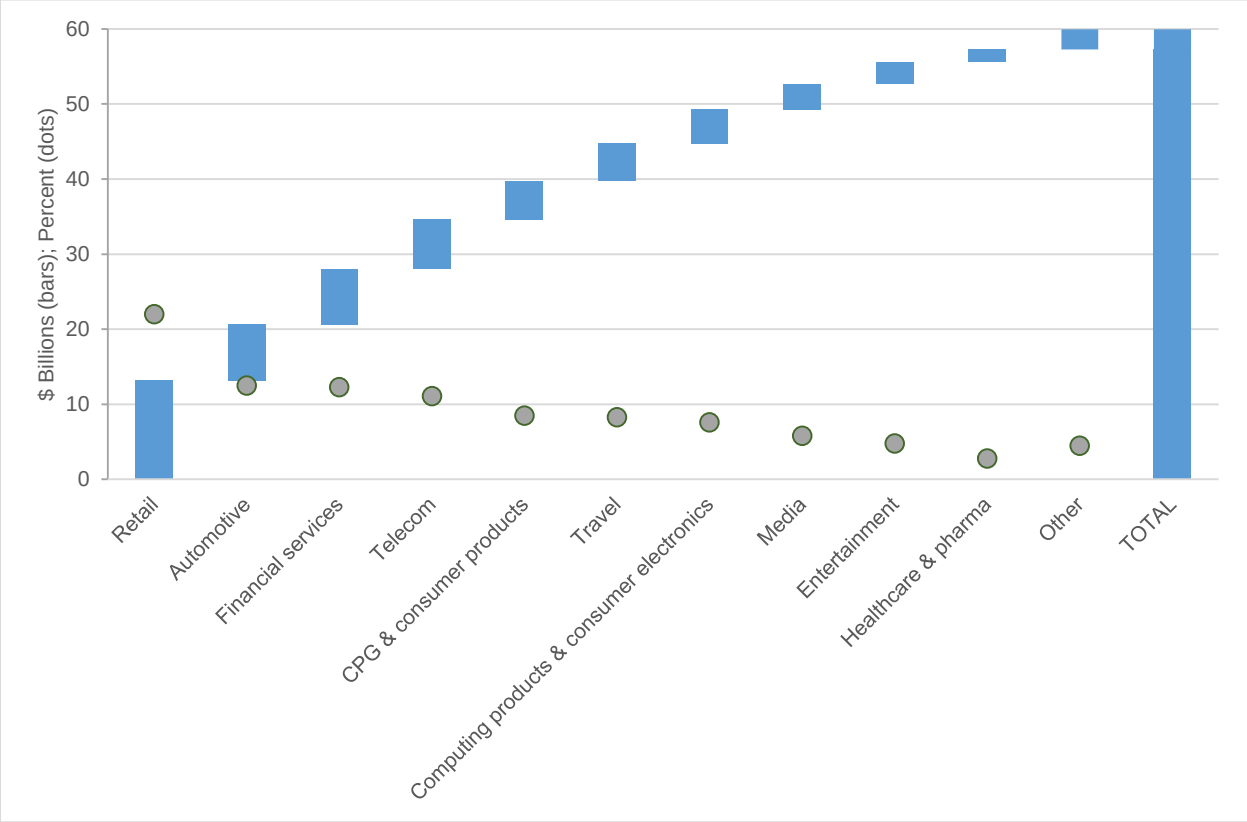
[110] Carlos Kirjner, "U.S. Internet and U.S. Telecom: Google Fiber - Have We Been Too Bearish?" (AllianceBernstein, December 9, 2015).

[111] See, for example, Scott Wallsten, "The Real Benefits of Gigabit Networks Have Nothing to Do with Speed" (Technology Policy Institute Working Paper, May 20, 2013), https://techpolicyinstitute.org/wp-content/uploads/2013/05/the-real-benefits-of-gigabit-n-2007574.pdf; T.C. Sottek, "Comcast Is Afraid of Google Fiber," *The Verge*, March 17, 2016, http://www.theverge.com/2016/3/17/11256318/comcast-is-afraid-of-google-fiber; Bill Snyder, "Google Fiber Competition Makes AT&T Cut Cost of Gigabit Service in Some Areas," *PCWorld*, October 5, 2016, http://www.pcworld.com/article/2989109/networking-hardware/google-fiber-competition-makes-att-cut-cost-of-gigabit-service-in-some-areas.html.

And the threat of entry from ISPs absent the proposed rules is real.[112] Despite a generally poor showing thus far, they are trying to improve their performance in digital advertising. Verizon purchased AOL, for example, as The Wall Street Journal put it, "to become a credible threat to Facebook Inc. and Google, the juggernauts of digital advertising."[113] Other ISPs have made other purchases for similar reasons,[114] and many advertise their digital advertising prowess.[115]

The market for advertising matters, of course, to companies and other organizations that need to advertise products and services. Figure 15 shows the distribution of digital spending by industry.

Figure 15: Spending on Digital Advertising by Industry, 2015



Source: Share of digital spending by industry is from eMarketer;[116] Spending in dollars is derived from share data and digital spending in Figure 8.

[112] Rani Molla, "ISPs Could Lose a Data Gold Mine," *Bloomberg*, April 7, 2016, http://www.bloomberg.com/gadfly/articles/2016-04-07/fcc-rules-could-hurt-isp-data-mining.
[113] Ryan Shields and Ryan Knutson, "AOL's Tim Armstrong Aims to Build Digital-Ad Empire at Verizon," *The Wall Street Journal*, March 30, 2016, http://www.wsj.com/articles/aols-tim-armstrong-aims-to-build-digital-ad-empire-at-verizon-1459330200.
[114] See, for example, Zacks, "Comcast Buys This Technology to Boost Digital Ad Platform," *Analyst Blog*, August 19, 2015, http://www.zacks.com/stock/news/186955/comcast-buys-this-technology-to-boost-digital-ad-platform.
[115] See also, for example, http://comcastspotlight.com/ and https://spectrumreach.com/.
[116] eMarketer. *Distribution of digital advertising spending in the United States in 2015, by industry*. http://www.statista.com/statistics/430376/digital-ad-spend-distribution-usa-by-industry/ (accessed May 20, 2016).

The retail industry is the biggest spender on digital advertising, representing 22 percent of all such spending in 2015, followed by automotive advertising at 12.5 percent. Retail margins are notoriously low—around three percent.[117] The data do not break automotive into its various components, but auto dealership pre-tax profit margins averaged about 2.3 percent in 2013.[118] In other words, some of the biggest spenders on digital advertising are businesses with low profit margins. If competition affects advertising prices, then these businesses should care a great deal about competition in the advertising market.

Any regulation that raises the costs of advertising and contacting customers will have a disproportionately adverse effect on smaller firms and new entrants.[119] This is especially true of internet advertising where established firms have data on their customers and visitors to their web sites, but new firms must purchase such data. As long as there is a market for customer data, entrants can begin competing relatively easily. If, however, regulation reduces the size of this market and increases costs, competition from new entrants will be reduced.

The FCC should spend some effort analyzing the advertising industry and exploring the effects of its rules on industries that buy advertising. The NPRM does not discuss this issue.

The Proposed Rules May Increase Consumer Costs and Decrease Entry

To the extent that the proposed rules bar entry into the advertising market, they may affect the way ISPs can fund their networks in the future. Blocking any particular source of revenue will make all remaining potential sources of revenue relatively more important. The FCC has already blocked ISPs from charging edge providers for guaranteed quality of service and other features. Reducing revenue potential from advertising would eliminate another potential source of revenues. The result would be continued reliance almost solely on direct payment by customers for broadband service. In other words, the rules risk locking in place the current industry funding structure: edge providers offer products to users without charge because they sell advertising while ISPs offer products in exchange for direct payment because they will be unable to sell advertising.

Making another source of revenue unavailable to ISPs may also block future entry. It is not inconceivable, for example, to imagine an ISP trying to emulate edge providers' approach and offer service without direct payment by the end user, instead funding costs through advertising. In fact, some providers are trying that model already. CellNuvo offers wireless service at no charge to the consumer, but provides data credits based on ads watched and information provided to the company via surveys.[120] Similarly, Freedompop allows subscribers to "earn additional broadband capacity, voice minutes, or text messages by performing specified actions with our third party advertisers (e.g., completing a questionnaire or purchasing a product or service)."[121]

---

[117] http://www.investopedia.com/ask/answers/071615/what-profit-margin-usual-company-retail-sector.asp; Even Walmart's profits rarely exceed 3.5% https://ycharts.com/companies/WMT/profit_margin.
[118] http://www.marketwatch.com/story/car-salesmen-arent-as-sleazy-as-you-think-2014-07-08
[119] Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Kluwer Academic Publishers, 2002, 78-79.
[120] https://cellnuvo.com/#phone-plans, last accessed May 20, 2016.
[121] https://www.freedompop.com/service_plan_terms.htm (under "special offers"), last accessed May 20, 2016.

The NPRM expresses concerns about offering such "financial inducements."[122] In particular, it asks whether exchanging information for service is permitted under the Telecommunications Act. We have no opinion on the legality of such practices. The economics, however, are not in question. Offering people more choices of ways to pay for service is unambiguously beneficial.

Such plans are likely to be marketed to price-sensitive consumers, who are also likely to be lower-income. The FCC worries that such plans "unfairly disadvantage low income and other vulnerable populations who are unable to pay for more expensive, less privacy-invasive service options."[123] Eliminating such options from the market, however, will not make the "less privacy-invasive" plans more affordable. The result would be either that the low-income people who chose those plans would have nothing or would have to pay more for their service than they would have otherwise, presumably giving up something else in exchange. Foreclosing this type of market entry, therefore, may have a disproportionate effect on lower income people and work counter to the FCC's longstanding goal of increasing adoption by the poor.

Consumers—including low-income consumers—may decide they do not like these kinds of broadband plans, but the FCC should not make that decision for them.

Conclusion

Privacy concerns are real and data breaches happen. Privacy protection and data security rules are justified. But those factors do not mean that stricter rules necessarily yield higher net benefits. Data is the currency that has funded much of the development of the internet. Restricting its flow has costs. Proposed rules should consider seriously both the costs and benefits of increasingly strict privacy rules. In this case, the question is not whether or not to have rules with which ISPs must comply. Rather, the question is whether the privacy regime that ISPs operated under when governed by the FTC was insufficient and whether the FCC's new rules yield incremental net benefits. The FCC does not address this fundamental question.

The FCC argues that ISPs have access to more data than do edge providers and therefore must follow stricter rules. The evidence, however, does not bear out that argument: the share of internet traffic that is encrypted is large and growing quickly and only a small minority of people use only a single ISP. In short, the FCC has not presented any evidence demonstrating that ISPs have more information than do edge providers.

Stricter rules, like those on data breach notification and opt-in requirements, would eliminate one potential source of revenues and put ISPs at a competitive disadvantage to edge providers in the digital advertising market. Reducing ISPs' ability to use targeted advertising for revenue helps ensure that end users will continue to pay directly for the costs of the network, whereas many edge providers are able to build out their services without direct charge to consumers. It also may foreclose entry options by ISPs hoping to follow the edge provider model and exchange broadband for data. Because those services are likely to appeal to the poor, this harmful effect on entry is likely to fall on low-income people, hurting the FCC's digital adoption agenda.

[122] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 259.
[123] Ibid., para. 261.

In short, the FCC should consider the many costs of its proposed rules and more explicitly consider whether consumers would be better off under the proposed rules or under rules more in sync with the rest of the internet.