Comments on Petitions for Reconsideration of Order

March 2017

Thomas Lenard and Scott Wallsten

409 12th Street SW ● Suite 700 ● Washington, DC 20024
Tel: (202) 828-4405 ● Email: info@techpolicyinstitute.org ● www.techpolicyinstitute.org

Before the FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS ON PETITIONS FOR RECONSIDERATION OF ORDER

Thomas Lenard and Scott Wallsten[*]

March 03, 2017

[*] Senior Fellow and President Emeritus and Senior Fellow and President, 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 FCC should reconsider its recently-passed privacy Order due to its failure to address serious issues raised in the comment period. In particular:

- The Order offers no evidence demonstrating that it would yield net incremental benefits over the FTC's rules or even that the Commission attempted to make such a determination. The Order fails to acknowledge any costs by not acknowledging benefits that flow from the creative use of information. It is therefore impossible for the Order to credibly claim the rules are beneficial or, as it claims, would "promote the virtual cycle of innovation."[1][2]

- The Order does not show that ISPs have access to more, and more sensitive, data than do edge companies. Instead, it compares ISPs' apples to edge companies' oranges and ignores evidence when convenient. For example, the Commission approvingly notes consumers' ability to switch search engines,[3] but does not acknowledge that more than 80 percent of Internet users report using the Internet at multiple locations.

- The Order inappropriately dismisses the privacy-enhancing effects of encryption by pointing out that much encrypted traffic is video from Netflix[4] while ignoring other evidence about the share of encrypted websites or search requests—not total traffic.[5]

- The Order continues to imply that privacy concerns harm broadband adoption,[6] yet ignores the empirical evidence contradicting this claim. The Order also does not acknowledge that if its claim were true it would apply equally to edge companies.

- The Order ignores the costs of creating entry barriers into the nearly $80 billion and growing digital advertising market. Entry barriers are likely to keep prices higher for advertisers by giving them fewer choices. At a bare minimum, the Commission should acknowledge this cost.

[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), para. 36.
[2] Ibid., para. 34.
[3] Ibid., para. 380.
[4] Ibid., para. 34.
[5] See, for example, 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.
[6] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 380.

Introduction

The Federal Communications Commission (FCC) recently adopted new privacy rules for Broadband Internet Access Service (BIAS) providers—also known as Internet Service Providers (ISPs).[7] Because the Order selectively ignores important questions and arguments that the Commission should have addressed prior to promulgating new rules, the Commission should reconsider those rules before allowing them to go into effect.[8]

Most importantly, the Order provides no evidence demonstrating that the new privacy rules would yield net—or, indeed, any—concrete benefits compared to the FTC's rules. The Order does not acknowledge that the rules would have any costs and implies no tradeoff exists between access to information and privacy. In reality, the creative use of information generates real benefits, and blocking data collection will reduce those benefits. That, of course, does not imply that privacy rules are unnecessary, but does imply that it is crucial to identify benefits of proposed rules and balance them with the costs of losing information.

Not only does the Order fail to acknowledge the tradeoff, it ignores the Commission's own—and, to our knowledge, its only—attempt to delve into the difficulty of the question. In particular, the NPRM and the Order do not mention the Commission's single workshop on privacy,[9] let alone attempt to derive any insights from it. Acknowledging a tradeoff is the first step towards determining whether the new rules would lead to incremental benefits beyond the rules that apply to other companies.

Contributing to this failure is the Order's selective use of evidence on several issues that commenters had noted in responses to the NPRM.

In particular, the Order does not demonstrate that ISPs have access to more, and more sensitive, data than other companies such that they require specific rules; falsely claims that privacy concerns harm broadband adoption; and ignores the costs of creating entry barriers to the digital advertising market.

The remainder of this comment discusses these issues in more depth.

The Order Fails to Acknowledge Costs of Reducing Access to Information

The key failure of the Order is its lack of acknowledgement that the rules are likely to have costs as well as benefits. This absence flows primarily from the Commission's not taking seriously the benefits that come from the use of data and, therefore, that reducing access to data has costs. Not acknowledging that reducing access to data has costs makes it possible for the Commission to

---

[7] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," Report and Order (November 2, 2016).

[8] These comments draw on Thomas Lenard and Scott Wallsten, An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking, May 25, 2016 (submitted as a comment on the NPRM).

[9] 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. https://www.fcc.gov/news-events/events/2015/04/public-workshop-on-broadband-consumer-privacy

claim the Order is beneficial under almost any circumstances. After all, if privacy rules have no costs, then stricter privacy rules will always only have net benefits.

The benefits of the use of data are well-documented,[10] and include supporting new online services, helping to protect against security threats, funding the creation of original content at Netflix (and presumably other content creators),[11] and notifying consumers of product recalls, to name just a few. 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 and other data-driven tools.

Arguably the closest the Order comes to recognizing that information has value and that its loss represents a cost is when it acknowledges that "opt-in imposes additional costs"[12] due to consumers' tendency to stick with the default choice. The Order dismisses this concern by claiming that "we find that opt-in is warranted" based on its "anticipat[ion] that many consumers, solicited by carriers incentivized to provide and improve access to their notice and choice mechanisms, will wish to affirmatively exercise choice options around the use and sharing of sensitive information." [13] The Order, however, provides no evidence of why it anticipates a particular consumer reaction or cite any research on how effective various incentives might be in encouraging consumers to change a default option.[14]

The benefits of data do not mean that privacy concerns are irrelevant or that privacy rules are unnecessary. But they do mean that costs and benefits of the rules affecting data availability and use must be considered carefully. Even when some benefits are not easily quantified, such as if privacy rules make consumers feel more secure, even an attempt at enumerating the two sides of the ledger facilitates good decision-making. The Order makes no attempt to do so, and ignoring the tradeoff leaves it with no way to think systematically about whether any benefits of the Order outweigh potential harms or if the Order is superior to the FTC's privacy rules.

The Order also omits other arguments or uses data selectively to dismiss arguments that do not support its conclusions, as discussed below.

---

[10] See, for example, Lenard and Rubin, "In Defense of Data."

[11] 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.

[12] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 194.

[13] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 194.

[14] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 177. Sensitive information typically refers to such data as financial data, health data, and data on children. The FCC's order is much more expansive and includes a customer's web browsing and application usage history. By including virtually all online behavior, it makes the distinction between sensitive and non-sensitive information almost meaningless.

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

A cornerstone of the defense of the Order is the claim that ISPs should face different privacy rules than all other firms in the economy. The Order contends, for example, that "BIAS providers can collect 'an unprecedented breadth' of electronic personal information."[15] The evidence, however, including that cited in the Order, does not demonstrate the claim to be true.

The Order's attempt to directly compare ISPs' and edge providers' access to data is flawed. The Order contends that

> …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. In contrast, a BIAS provider sees 100 percent of a customer's unencrypted Internet traffic.[16]

Comparing access to a percent of web pages to the share of unencrypted traffic is meaningless. The Order does not provide any reason to believe that "100 percent of…unencrypted traffic" (which is an increasingly small share of all traffic) reveals more, or more sensitive data, than "25 percent of web pages."

The Order also does not properly consider increased encryption, the use of multiple ISPs, or where data breaches have actually occurred.

Encryption

Encryption is increasingly becoming the norm across the Internet. Because ISPs cannot see the contents of encrypted traffic, the Order acknowledges that "encryption can significantly help protect the privacy of consumer content from BIAS providers."[17] Georgia Tech professor Peter Swire, et al, argue in their report on ISPs and privacy, that "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."[18] The Order does not directly address the Swire, et al argument and dismisses the role of encryption based on assertions that do not withstand scrutiny.

---

[15] National Telecommunications and Information Administration, "Exploring the Digital Nation: Embracing the Mobile Internet," October 2014, https://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_embracing_the_mobile_internet_10162014.pdf.

[16] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 30.

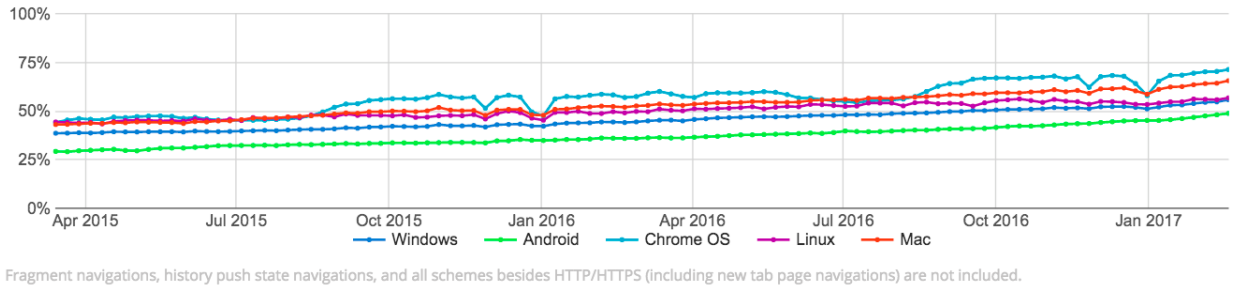
[17] Ibid., para. 33.

[18] 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.

The Order argues that ISPs can observe certain metadata when the connection is encrypted, and metadata can sometimes be combined to reveal some other information.[19] To the extent both claims are true, however, the FCC does not explain why that information is necessarily more sensitive than information observed by other large platforms, why the ability to combine data is more of a concern with metadata collected by ISPs than with data collected by other edge providers, and why the FTC rules are insufficient.

Additionally, the Order suggests that the growing encrypted share of Internet traffic may be misleading because so much traffic is Netflix video.[20] This observation is correct. However, the Order ignores other data showing a steady overall trend in encryption, not just in traffic. Some data show, for example, increased encryption by industry, and other data show the growing share of connections and websites—not just the share of traffic—that are encrypted. Google's latest transparency report, for example, shows that even just from the time the Order was released through February 18, 2017 the share of web pages loaded over encrypted connections increased by three to five percentage points to over 50 percent for all platforms tracked except Android, which was at 49 percent (Figure 1).

Figure 1: Percent of Pages Loaded Over HTTPS



Source: Google Transparency Report.[21]

People Access the Internet from Multiple Locations

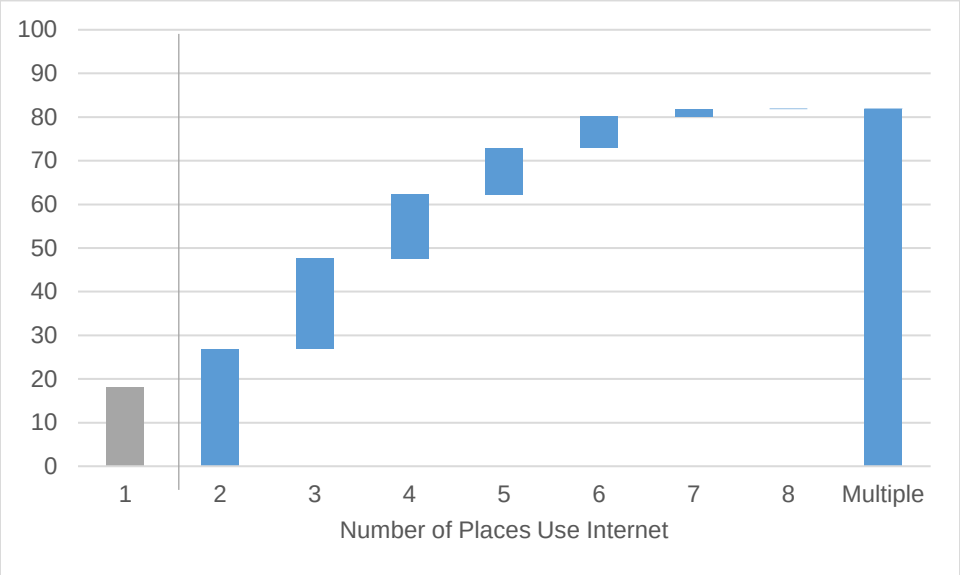
The Order seems to back down from the NPRM's strong claim that consumers cannot avoid a particular ISP's network but can "instantaneously" switch among edge providers. Instead, the Order argues that consumers face high switching costs in choosing another ISP.[22] It ignores, however, the point that consumers access the Internet from multiple locations and, therefore, use many ISPs.

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

[19] Thomas M. Lenard and Scott Wallsten, "An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking" (Technology Policy Institute Working Paper, May 25, 2016), fig. 12, https://techpolicyinstitute.org/wp-content/uploads/2016/05/Lenard_Wallsten_FCCprivacycomments.pdf.
[20] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 34.
[21] https://www.google.com/transparencyreport/https/metrics/?hl=en, accessed March 1, 2017.
[22] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 36.

logged in to the same email account, using the same e-commerce sites, and exploring the world with the same search engine.[23] Indeed, less than 20 percent of internet users report using the internet at only a single location,[24] more than 80 percent report using it at least two locations, and more than half in at least three locations (Figure 2).

Figure 2: 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.[25]

Again, the key question is whether ISPs should be treated differently from edge providers. This information suggests that they should not. Applying stricter privacy rules to one over the other is arbitrary.

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

The Order continues to assert that the Commission has found that privacy concerns hinder broadband adoption[26] despite its "finding" being based on suppositions and hypothetical scenarios rather than empirical evidence.[27] Even if this were true, however, it should apply also to edge companies, and is thus unrelated to the claim that ISPs deserve special attention. Empirical evidence, moreover, suggests that privacy concerns have not hindered Internet adoption or use.

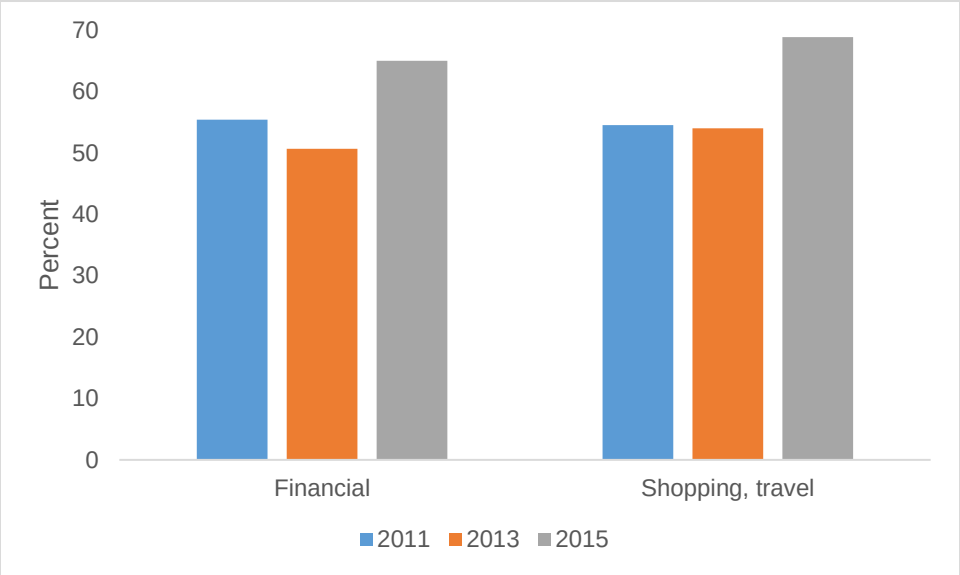
---

[23] Lenard and Wallsten, "An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking," 17.
[24] Ibid., 18.. 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.
[25] Share is of respondents at least 15 years old who reported using the internet anywhere and answered all questions about where they use it.
[26] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 380.
[27] For a full discussion, see Lenard and Wallsten, "An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking," 19.

An NTIA report noted "only 1 percent of households expressed privacy concerns in both 2011 and 2012 as their primary reason for not using the internet at home…."[28] A subsequent July 2015 Computer and Internet Use Supplement to the Current Population Survey found that less than one-half of one percent of non-adopters noted privacy concerns as the key reason they did not use the internet.[29] Similarly, a 2015 Pew survey found less than one percent of respondents who did not own smartphones cited privacy concerns as a reason.[30]

Additionally, the evidence suggests that privacy concerns have not prevented people from increasing their use of the Internet for sensitive transactions. Data from the July 2015 CPS Computer and Internet Use supplement, for example, show more people engaging in financial transactions and online shopping in 2015 than in any previous year (Figure 3).

Figure 3: 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

Privacy concerns are important, and it is possible that internet adoption and use would be even more robust were internet users less concerned about privacy. However, the FCC has not produced or cited evidence showing that to be the case. The available data seem to show the contrary.

Data Breaches by Industry

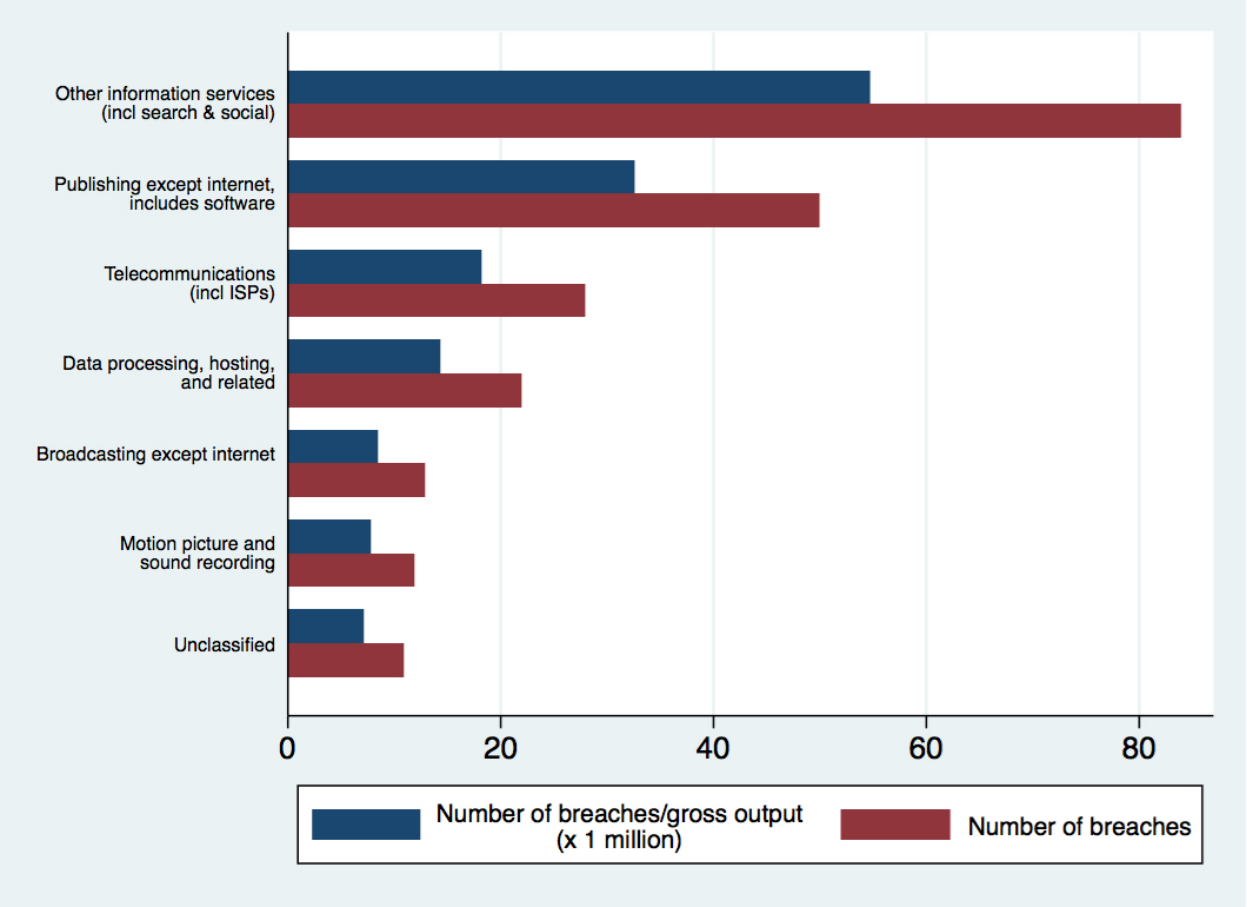
One reason to target a particular industry might be if it has been particularly prone to damaging data breaches. Available information suggests that ISPs are no worse—and better than—several

[28] National Telecommunications and Information Administration, "Exploring the Digital Nation: Embracing the Mobile Internet."
[29] Analysis of July 2015 Current Population Survey Computer and Internet Use Supplement.
[30] 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/.

other industries. As we showed in our earlier filing, industry data for 2010-2015 show 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.[31] The industry classified as "information services," which includes ISPs and edge companies like search and social media, and is fifth on this list.

Within "information services", "other information services," which includes edge companies, has the highest number of breaches, followed by "publishing, except internet, including software."[32] Telecommunications, which includes ISPs, is third (Figure 4).[33]

Figure 4: 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]

[31] See Lenard and Wallsten, p. 11.
[32] "Publishing, except internet" includes online gaming companies, which account for the majority of data breaches in that subsector.
[33] Lenard and Wallsten, p. 12
[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 4.
http://www.bea.gov/industry/gdpbyind_data.htm

Thus, the data show 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 do not support a more rigorous focus on ISPs.[36]

The Effects of the Order on Competition

The Order does not address the question of how it might affect competition in the digital advertising market even though it was raised during the comment period. To the extent the Commission addresses this market at all it is to imply that restricting targeted advertisements could be a benefit.[37] But digital advertising revenues are large and growing. Total media advertising spending was expected to be about $200 billion in 2016,[38] with digital spending at $77 billion in 2016, up from $67 billion in 2015.[39] Creating barriers to entry in this market will create only costs.

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.[40] 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.

While consumers may not be affected directly by the market for advertising, it matters to companies and other organizations that need to advertise products and services.[41] 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.[42] The data do not break automotive into its various components, but auto dealership pre-tax profit margins averaged about 2.3 percent in 2013.[43] In other words, some of the biggest spenders on digital advertising are businesses with low profit

---

[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] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," paras. 298, 366, 379.

[38] Lenard and Wallsten, "An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking," fig. 12.

[39] Forrester Research, and Business 2 Community. *Digital marketing spending in the United States from 2014 to 2019 (in billion U.S. dollars)*. Via Statista (accessed March 1, 2017).

[40] 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.

[41] Lenard and Wallsten, p. 34.

[42] 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.

[43] http://www.marketwatch.com/story/car-salesmen-arent-as-sleazy-as-you-think-2014-07-08

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.[44] 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, the effect will be to reduce competition from new entrants.

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, and restricting its flow has costs. The Order fails to acknowledge the benefits of data, let alone try to estimate the costs of restricting access to it and balancing those with any benefits from stricter privacy rules.

The failure to identify and balance costs and benefits is consistent with several errors and omissions in the Order. In particular, The Order

- does not demonstrate that ISPs have access to more data than edge providers;
- does not fully or properly consider the effects of growing encryption;
- ignores the implications of the observation that only 20 percent of Internet users sign on from only a single location;
- incorrectly asserts a link between stricter privacy rules and increased broadband adoption; and
- ignores the evidence that firms other than ISPs are more prone to data breaches.

For all these reasons, the FCC should take this opportunity to reconsider the privacy Order.

[44] Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Kluwer Academic Publishers, 2002, 78-79.