August 18, 2016

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: Ex Parte Presentation, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106

Dear Ms. Dortch,

On August 16, 2016, Maria Kirby, Debbie Matties, and the undersigned of CTIA met with Claude Aiken of the Office of Commissioner Clyburn and Amy Bender of the Office of Commissioner O'Rielly to discuss the above-referenced proceeding. On August 18, 2016, we met with Travis Litman and Jennifer Thompson of the Office of Commissioner Rosenworcel and Nick Degani of the Office of Commissioner Pai regarding the same. During the meetings, CTIA discussed the importance of harmonization of privacy policy across the internet ecosystem; aligning data breach and data security provisions with existing state law; use of de-identified data; and payment models that vary by consumer privacy preferences.

With respect to harmonization, we noted that domestic and international policy developments call for privacy rules that center equal treatment of broadband companies and other companies operating on the internet. The Obama Administration carefully highlighted the need for consistency in its 2012 Privacy Blueprint and Consumer Bill of Rights. The U.S. government reinforced this stance in its EU Privacy Shield negotiations, maintaining that the FTC standard, in combination with law focusing on sensitive data where appropriate and robust enforcement, provides strong protection for consumers. A different standard

from the FCC for only some companies handling internet data will undermine that advocacy.

We also highlighted how longstanding state laws point the way on data breach notification. Where there is risk of consumer harm, internet service providers (ISPs) should notify consumers, which will ensure that customers focus their attention to notices that are most likely to affect them directly. The breach notification rule should provide a reasonable time to send notices to allow for investigation of the breach and a determination of which customers were affected. If the notification is sent too quickly, consumers may get incomplete or inaccurate information, and companies may not have enough time to fix the breach or help law enforcement find the perpetrators. The FTC recommends that the FCC allow for 30-60 days, the shortest time under state law, and CTIA agrees with this approach.

Our discussion of de-identified data – data from which personal identifiers is removed – also drew from FTC and other agency guidance. Companies can choose to de-identify data to protect privacy while still allowing the data to provide significant societal and consumer benefits. Under the FTC guidance, technical measures to de-identify data must be reasonably robust, and these measures must be accompanied by administrative measures. Specifically, companies must commit to not re-identify data and require downstream recipients of de-identified data to do the same. Many other companies, including mobile app stores and advertising networks, protect consumer privacy by using random identifiers to de-identify data.

Finally, we briefly noted that allowing consumers a variety of options regarding whether to receive a discount on broadband service in exchange for personalized advertising should be preserved. Hybrid payment models have been in commerce for centuries, including advertising supported magazines, grocery store loyalty programs, and app-based discount programs for retail establishments. Many internet companies rely on use of consumer data as their sole source of income, like search engines and social networks. Such offerings can lead to significant cost savings for all consumers, enable more valuable

services for consumers, and mirror much of the economic activity that consumers expect. On this point, we provided a copy of a recent report by the Information Technology & Innovation Foundation, titled "Why Broadband Discounts for Data are Pro-Consumer," which is attached to this filing.

Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed in ECFS and provided to the Commission participants. Please do not hesitate to contact the undersigned with any questions.

Sincerely,

/s/ Scott K. Bergmann

Scott K. Bergmann
Vice President, Regulatory Affairs
CTIA

Attachment

Cc: Claude Aiken
Amy Bender
Nick Degani
Travis Litman
Jennifer Thompson

Why Broadband Discounts for Data Are Pro-Consumer

BY DOUG BRAKE | AUGUST 2016

A prohibition on privacy-based discounts would be a remarkably paternalistic departure from accepted practice throughout the economy and would hurt consumers and slow broadband adoption.

This past April, the Federal Communications Commission (FCC) proposed a sweeping new privacy regime for broadband providers, seeking to impose additional restrictions on use of customer data above and beyond the privacy protections that the Federal Trade Commission historically has applied to this sector. Attention has focused on whether or to what extent broadband providers can offer discounts or inducements in exchange for permission to use consumer information commercially, even if the information is anonymized. Some critics, framing these discounts as "pay-for-privacy," have advocated that they be prohibited in the FCC's forthcoming rules. Such a ban would be bad policy. A prohibition on price differentiation would be a remarkably paternalistic departure from commonly accepted practice throughout the economy and would hurt consumers and slow broadband adoption.

These types of discounts are especially common in industries with relatively high up-front costs and relatively low costs to serve each additional user, as is the case in software, web-based services, and Internet access. Although broadband is too costly to provide for these discounts to bring the cost to zero, as is often the case with online services like webmail, this does not change the fact that price differentiation is unquestionably welfare-maximizing for consumers and the economy.

OVERVIEW OF PROPOSED FCC PRIVACY REGULATIONS

The debate over privacy-based discounts warrants some context. The FCC has proposed extensive rules which would apply narrowly to broadband access providers. At a high level, the FCC put forth for discussion a three-tier consent scheme to constrain how broadband

providers could use customer data and to stipulate what type of permission they must get from consumers before doing so. This framework consists of (1) implied consent for data used in providing broadband service, (2) opt-out consent for marketing "communications-related" services, and (3) opt-in consent for any other uses of data.[1] The entire regulatory scheme is explicitly structured around what business practices broadband providers can and cannot employ. The FCC's proposed privacy regime does a poor job of balancing the goals of innovation and productivity with other policy interests, and ITIF has consistently opposed the entire FCC privacy undertaking.[2]

A question asked by the FCC in its proposed rules is whether business practices that offer consumers financial inducements, such as lower monthly rates, in exchange for consent to use and share information should be allowed.[3] The FCC rightly recognized that "[i]n the broadband ecosystem, 'free' services in exchange for information are common."[4] Yet some advocates are calling on the FCC to prohibit these practices.

The remainder of this section provides additional context and describes drawbacks of the FCC's overall approach. The balance of the report then focuses narrowly on the financial inducement question.

Sector Specific Rules Are Not Justified

In order to justify the FCC's sector-specific rules, one would expect an unusually high risk of consumer harm from consumer broadband data being shared inappropriately. After all, the only sector-specific privacy rules are for areas of the economy, such as health care or financial services, where there exists a heightened risk of harm from the disclosure of sensitive personal information. But, as a factual matter, that heightened risk does not exist with regard to broadband providers: Their access to data is neither unique nor comprehensive.

Between the rapidly growing use of encryption, availability of virtual private networks and proxy services, and consumers use of multiple networks throughout the day, no one broadband provider has anything near comprehensive access to consumer data.[5]

Broadband provider access to data is simply not unique. In fact, large amounts of similar consumer data are already available to anyone interested in buying it from a broker.[6] The proposed rules thus would lead to the strange and market-distorting result where broadband providers would not be allowed to share or use the exact same information that is readily available to others.

Moreover, all major broadband providers already offer consumers the ability to opt out of existing targeted advertising programs, an important and often-overlooked point.[7] In line with FTC guidance, broadband providers all offer notice of the data that is collected and the option for consumers to opt out of practices they are uncomfortable with.[8] Contrary to the FCC's assertions, the truth is users will have no more and no less "control" over how companies use their broadband data under the proposed rules. What will change, however,

is the ability of ISPs to responsibly experiment with new ways of supporting the expensive deployment and maintenance of broadband networks.

The FTC Model Better Balances Privacy with Other Values, Such as Innovation

Any new regulations should recognize there is a balance between the benefits additional sharing and use of data and the risk of privacy harms.[9] The research of Catherine Tucker at MIT has shown the light-touch privacy regime in the United States is a significant factor in why this country leads in the Internet economy compared to regions with more restrictive privacy regimes, such as the European Union.[10]

We should prefer the FTC model as simply superior to what the FCC has proposed in supporting data innovation. The FTC oversees fair competition and has broad authority under Section 5 of the Fair Trade Act to take enforcement actions against unfair or deceptive trade practices.[11] The FTC also offers specific guidance when it comes to privacy, having put forth a single, comprehensive framework guided by three overarching principles: privacy by design, consumer choice, and transparency.[12]

When it comes to privacy, most Americans favor voluntary standards and are willing to make trade-offs around sharing their data in exchange for concrete benefits.

By allowing flexibility for industry to develop best practices within these guidelines, and stepping in after the fact where problems develop, the FTC does not have to predict the direction technological advancements or changes in business practices will take us. This allows firms to internalize or outsource different functions in fast-paced industries, focusing on efficiency rather than compliance. This type of privacy oversight, with rules that apply an even, light-touch approach to different actors, provides a better environment for dynamic competition to occur across platforms.

The FCC proposal would take us in a different direction. At a high level, it contemplates a requirement that broadband providers obtain affirmative, opt-in consent from consumers before using or sharing even non-sensitive data for "non-broadband" purposes, such as targeted advertising.

The FCC's Options

When it comes to promoting innovation and productivity growth, the best course would be for the FCC to abandon its privacy proceeding, announce that broadband privacy practices are not a common-carrier activity, and leave broadband privacy for FTC oversight. Unfortunately, this appears unlikely.

Second best, the FCC could align its regulations with the best practices developed by the FTC, tailoring the type of consent required to the sensitivity of the data being shared, rather than the use it is being put to. In comments on the proposed rules, the FTC staff itself recommended the FCC focus on the sensitivity of data.[13] Under this approach, financial inducements would be allowed, but may not be necessary, considering many users would be comfortable with default participation.

If the FCC unwisely forges ahead with the rules as proposed, then the question of discounts-for-data become important, as broadband providers may have to share some of the value created by use of this data with consumers in order to induce broader

participation. Such discounts may add to the total costs of providing broadband compared to an opt-out-based nudge toward sharing. Regardless, discounts based on sharing data would be an efficient way to find those willing to participate in data sharing programs, and experiments with these programs should be freely allowed.

PRICING BASED ON CONSUMER CHOICE REGARDING DATA IS GOOD POLICY

Broadband providers in some markets are experimenting with discounts for users who opt in to sharing broadband data. Most notably, AT&T, with its "Internet Preferences" program, offers a $30 discount for allowing its analytics platform to access the webpages visited, time spent on each, the links or ads consumers see and follow, and the search terms consumers enter.[14] Customer-identifiable data would not be shared with third parties. Other broadband providers are at least exploring such programs, whether or not they intend to implement any time soon.[15]

Privacy Preferences Vary

In considering the value to consumers of such a program, it worth recognizing that consumer privacy preferences vary considerably. Allen Westin, the late emeritus professor of public law and government at Columbia University, performed several foundational surveys that helped form an understanding of the American public's attitude toward privacy. He formulated three general groups of people with different stances toward privacy values.[16]

"Privacy Fundamentalists," according to Westin's surveys, represent about a quarter of the population.[17] This group places an especially high value on personal privacy and is distrustful of business or government use of their data. These individuals favor strong protections of privacy rights and tend to refuse access to their information. Most privacy advocates pushing for a ban on privacy-based discounts surely fall into this group and tend to argue that most Americans do too.

Westin also identified what he called the "Privacy Unconcerned."[18] This group represents about a fifth of the United States, and has little concern for privacy. They have no problem sharing their information and don't understand "what the privacy fuss is all about."[19]

Westin calls the largest group, representing 55 percent of U.S. citizens, "Privacy Pragmatists."[20] Westin explains, the "[p]ragmatists favor voluntary standards over legislation and government enforcement" and are willing to make tradeoffs around sharing their data, especially if expanded use of the data is beneficial to society.[21]

This general fact, that the lion's share of consumers are willing to trade their data if there are benefits to doing so—either to them or to society—is well recognized by other researchers. As Pew Research Center put it in a recent report, "[m]ost Americans see privacy issues in commercial settings as contingent and context-dependent…[and] many Americans are willing to share personal information in exchange for tangible benefits…."[22] Pew's research shows remarkable diversity in preferences, and while many are concerned

about how their information is shared, others are quite happy to trade even sensitive data for benefits in the right circumstances.[23]

Flat bans on providing discounts in exchange for data, like the one proposed by the Open Technology Institute (OTI), assume everyone shares their fundamentalist outlook.[24] On the other hand, allowing these differentiated pricing programs to go forward recognizes customers are competent enough to decide where they stand on these trade-offs and that many consumers, of all income levels, will choose to save money. Effective notice and choice should continue to be the guiding light when it comes to privacy discounts, not flat bans.

Nearly 90 percent of U.S. shoppers use some kind of loyalty discount card, which offer financial inducements in exchange for data, often for essential goods like food.

Discounting and Price Differentiation Is Pervasive, Especially on the Internet

Offering similar services at different prices for different classes of customers—what economists call "price discrimination"—is extremely common and widely accepted as welfare-maximizing in most circumstances. Harvard Law Professor Einer Elhauge explains the pervasiveness of price differentiation well:

> [Price discrimination] is routine even in highly competitive markets, including hotels, computers, automobiles, books, clothing, groceries, restaurants, telecommunications, and the vast range of other products that offer coupons, rebates, student or senior discounts, quantity discounts, or different prices at different times or places. Indeed, it is hard to think of industries without price discrimination…[25]

Users generally differ according to their ability and willingness to pay for the same or similar services. Price differentiation is generally progressive, as it helps make the service cheaper for those less willing or able to pay when those willing to pay more shoulder more of the total costs of the system.

Discounts of different forms in exchange specifically for user data is a fundamental premise of many online services. Perhaps most familiar is the "freemium" model, where companies looking to gain scale will offer one version of their product for "free" (usually in exchange for user data), and an enhanced version for a fee. Free webmail, free social networking, and free search are just a few of the most obvious examples of this familiar and time-tested trade-off.

Without the ability of companies to use data to target ads, the Internet as we know it would be a shell of itself, not the pervasive, progressive force it is. Targeted ads that are relevant to a particular user generate more than twice the revenue of non-targeted ads and are, and will continue to be, an important source of revenue for the Internet ecosystem, particularly the so-called "long tail" of small websites supported by ad revenue.[26]

Broadband Privacy-Based Price Differentiation Is Similar to Other Discounts

Broadband providers offering a discount for access to user data is not different from those commonly enjoyed online. Of course, price differentiation is already built into broadband

services, in the form of different speed tiers on wired networks and different data plans on mobile networks. Privacy simply offers another value that customers can consider.

One obvious difference is that the discount in the broadband context generally does not bring the price down to zero. The expense involved in providing high-speed Internet access to the home is not exceeded by the value of consumers' browsing data, as can be the case in the context of apps or web services. This is why, for example, AT&T's Internet Preferences program offers a $30 discount rather than free service.

Others have shown collecting data and targeting advertising can allow for broad deployments of free, public WiFi. Beyond WiFi deployments in cafes and coffee shops (which also collect user data), both New York City and Kansas City have deployed kiosks that provide a free Internet connection.[27] LinkNYC in New York was widely celebrated as offering fast, free Internet, but it does so on the condition that browsing information is shared with third parties for targeted adverting.[28] This service would likely be illegal under the FCC's proposed rules, despite being tremendously beneficial to tourists, those unable to pay for a connection at home, or even New York residents out and about.[29] These services show there is a business model that can give free Internet access to customers who are willing to trade their privacy (if the FCC will allow it).

Critics of these sorts of deals argue that broadband is special, because it is an "essential service," and customers should not be allowed to share their data in exchange for a discount (even if the data is not shared with third parties and only computer algorithms ever "read" it), lest low-income individuals feel forced to take the deal. Better everyone receives the same service, even if it is more expensive, than have one customer pressured into a discount.

Whether a service is "essential" is not determinative in developing privacy guidelines or regulations. Rather, the importance of the service is one factor to be considered along with the advantages of additional data sharing and use. In fact, other "essential" services enjoy far more flexible data sharing compared to the restrictions proposed by the FCC, even in monopoly utility circumstances.

Consider water utilities. While water use is certainly not as sensitive as broadband data, there are not restrictions on the sharing of water use information. Some utilities in California publicly published names, addresses, and gallons of water used by "excessive" consumers in an attempt to shame over-use during droughts.[30]

Electric utilities have access to smart grid data, which can reveal personal behavior patterns and granular information about what appliances are used and when.[31] There are no sector-specific privacy regulations for the smart grid—privacy oversight here, like most of the economy, is left to the FTC, particularly to monitor abuses.

The Department of Energy (DOE) developed a set of voluntary best practices for smart grid operators. This voluntary code of conduct was the result of a 22-month multi-stakeholder effort that was facilitated by the DOE Office of Electricity Delivery and Energy

Reliability in coordination with the Federal Smart Grid Task Force.[32] Recognizing the need to "encourage innovation" and the benefits of sharing this type of data does not require consent for sharing of reasonably anonymized or aggregate data and does not discourage any sort of discounting or inducements for sharing data.[33] TRUSTe has developed a privacy certification program for smart grid providers and related products that is significantly less onerous than the FCC's proposed privacy rules, allowing for sharing of data largely on an opt-out basis.[34]

Also salient to the debate is food. Food is clearly more essential than broadband, yet discount cards that track grocery shopping habits are commonplace. Nearly 90 percent of U.S. shoppers at all income levels happily use some kind of loyalty discount card.[35] These cards offer strong financial inducements—discounts on purchases or other rewards—in exchange for data collection, data which is often sold to third parties. Most are quite happy to make this trade-off because they know from experience that there is no consumer harm. Other areas where privacy trade-offs are allowed for important services abound, such as credit cards or other financial instruments.

Banning discounts to make broadband more affordable based on a personal choice about how much one values one's privacy is a remarkably elitist, paternalistic view.

Advocates also claim a ban is justified because of the reduced number of choices of broadband providers compared to online services where privacy-based trade-offs and discounts are commonplace. First of all, these arguments are built on a shaky factual foundation of the competitive landscape for broadband access, as they often rely on the FCC's arbitrary 25 Mbps threshold.[36] Second, there is no way in which consumer choice, in the form of a simple opt-out mechanism—which providers already offer—does not cure this "choice" question. The minority of consumers who are unusually privacy sensitive have the ability and incentive to opt out of data collection programs they are not comfortable with. Similarly, in the context of financial inducements, consumers have the choice to not take the discount offered and pay the full price the service would normally be offered at.

Discounts Benefit Consumers

This should go without saying, but discounts lower the cost to consumers, broadening the number of consumers who can afford high-speed broadband. Privacy fundamentalists should not prevent those who are willing to give up data on their browsing habits from doing so, especially when it might make the difference in gaining access. Furthermore, given the network effects of Internet participation, gaining additional users benefits the Internet ecosystem overall.

ARGUMENTS AGAINST EXPERIMENTATION WITH PRIVACY DISCOUNTS ARE UNFOUNDED

OTI's Eric Null argues these price-differentiation programs are unfair, writing "[t]his kind of coercion is the precise design of pay-for-privacy schemes: charge consumers a hefty premium, untethered to the actual value of the data, to protect their privacy so they will have a difficult time justifying the additional cost."[37]

Advocates like Null want to have their cake and eat it too. They want ubiquitous, undifferentiated service for everyone, but they don't want to pay for it. They bemoan the

price of high-speed broadband as too high for low-income Americans, but seek to close off opportunities to put downward pressure on price. Banning discounts to make broadband more affordable based on a personal choice about how much one values one's privacy is a remarkably elitist, paternalistic view the FCC should not entertain.

Moreover, this position is not based on realistic concerns, but rather policymaking by worst-case scenario. Advocates envision a race to the bottom, where broadband providers design pricing practices to extract the maximum data possible from those least able to forego a discount.[38] They couch their argument in vague terms of inequality, claiming that these programs make privacy a "luxury good," and coerce low-income consumers into giving up their privacy without even acknowledging that a fair discount would benefit these consumers most of all.

Advocates claim these programs coerce low-income consumers into giving up their privacy, but don't acknowledge that a discount would benefit these consumers most of all.

This vision is a straw man. Instead of policy by worst-case scenario, we should consider the actual facts of how these programs have been implemented to date. Advocates tug at heartstrings with visions of privacy-deprived poor, when in reality, AT&T, where it has trialed this mechanism, has only implemented opt-in privacy based discounts *on its most expensive product.* For the company's GigaPower high-speed fiber-to-the-home service, this discount option is available, but for lower-speed, U-verse options, there are no financial inducements offered. Perhaps, instead of harvesting information from low-income Americans, AT&T is attempting to serve more effective advertisements to America's wealthy, who are much more likely to buy goods and services and online.

Most consumers happily give up some data in exchange for services online. Those at OTI may choose specialized, privacy-preserving search and email services, or forego popular social networks. But they are in the minority. Many happily use mainstream services based on sharing data, and many likely would be happy to take a discount on their broadband bill. They have no legitimate claim to speak for all consumers—consumers should be empowered to choose whether a privacy-based discount is right for them. Banning discounts for data would remove beneficial choices for the majority of Americans who are either unconcerned about their privacy or pragmatists willing to make trade-offs.

CONCLUSION

The FCC should recognize that privacy-based discounts clearly have the potential to benefit consumers and refrain from limiting the use of this practice by broadband providers. These mechanisms can make service cheaper for those willing to allow providers to conduct machine-based analytics on some of their data; they would put downward pressure on price for consumers who do not want to take the discount; and they would, on the margin, add users to the broadband ecosystem. Advocates' calls for prohibitions are paternalistic and not well grounded in reality.

ENDNOTES

1. *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 31 FCC Rcd 2500 (2016).
2. *See* Doug Brake, Daniel Castro, & Alan McQuinn, ITIF, "Broadband Privacy: The Folly of Sector-Specific Regulation" (2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf; Doug Brake, Daniel Castro, & Robert D. Atkinson, ITIF, "The FCC's Privacy Foray: Privacy Regulation Under Title II" (2015), http://www2.itif.org/2015-fcc-privacy.pdf; Doug Brake, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of ITIF," WC Docket No. 16-106, *available at* http://www2.itif.org/2016-broadband-privacy-comments.pdf?_ga=1.25209844.812486504.1449157248; Doug Brake, "The FCC's Privacy Ruse," *Forbes* (April, 2016), http://www.forbes.com/sites/realspin/2016/04/27/the-fccs-privacy-ruse/#1c47825b10aa; *House Committee on Energy and Commerce Subcommittee on Communications and Technology: Hearing on FCC Overreach: Examining the Proposed Privacy Rules* (2016) (testimony of Doug Brake, telecommunications policy analyst, ITIF).
3. Ibid at para. 259.
4. Ibid at para. 260.
5. *See* Peter Swire, et al, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,* The Institute for Information Security & Privacy, Georgia Tech, Feb 2016, http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.
6. As Jules Polonetsky, head of the Future of Privacy Forum, has put it, "[t]oday, data has been democratized." Jules Polonetsky, "Broadband Privacy and the FCC: Protect Consumers from Being Deceived and from Unfair Practices," *Future of Privacy Forum* (March 2016), https://fpf.org/2016/03/11/13938/.
7. *See* Doug Brake, Daniel Castro, & Alan McQuinn, Information Technology and Innovation Foundation, Broadband Privacy: The Folly of Sector-Specific Regulation, (2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf.
8. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
9. On this balance, *see* Avi Goldfarb & Catherine Tucker, "Privacy and Innovation," in *Innovation Policy and the Economy, Volume 12* U. of Chicago Press (2012), 65-89.
10. Catherine Tucker, "Empirical Research on the Economic Effects of Privacy Regulation," 10 *J. on Telecomm. & High Tech. L* 265 (2012) *available at* http://jthtl.org/content/articles/V10I2/JTHTLv10i2_Tucker.PDF
11. 15 USC § 45.
12. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, *supra* note 8.
13. Staff of the Bureau of Consumer Protection of the Federal Trade Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of FTC Staff," at 22, WC Docket No. 16-106, available at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.
14. "U-verse with AT&T GigaPower Internet Preferences," *AT&T*, accessed August 11, 2016, https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1011211.
15. *See* Francis M. Buono, "Letter to Marlene H. Dortch re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (ex parte notice, August 1, 2016) *available at* https://ecfsapi.fcc.gov/file/10802205606782/Comcast%20Ex%20Parte%20--%20WC%20Dkt%20No%2016-106%20--%207-28%20WCB%20Meeting.pdf.

16. *For example, see,* Alan F. Westin "The Public's View of When Privacy Self-Regulation Is Appropriate: 'Whatever Works' The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues," *NTIA*, *available at* https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. Ibid.
22. Lee Rainie and Maeve Duggan, "Privacy and Information Sharing" (Pew Research Center Internet, Science & Tech, January 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.
23. Ibid.
24. *See* Eric Null, "Comcast Wants You to Empty Your Wallets to Protect your Privacy" *Open Technology Institute,* Aug 5, 2016, https://www.newamerica.org/oti/blog/comcast-wants-you-empty-your-wallets-protect-your-privacy/.
25. Einer Elhauge, "Why Above-Cost Price Cuts To Drive Out Entrants Are Not Predatory—and the Implications for Defining Costs and Market Power," Yale Law Journal, v. 12, 2003, p. 733.
26 . "Study finds behaviorally-targeted ads more than twice as valuable, twice as effective as non-targeted online ads," Network Advertising Initiative, press release, March 24, 2010, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf.
27. *See* Stacey Higginbotham, "In Kansas City you trade your data for Wi-Fi," *Medium* (May 2016) https://medium.com/@gigastacey/in-kansas-city-you-trade-your-data-for-wi-fi-5ef26e8bed54#.8ddlm3pvs; Kaveh Waddell, "Will New York City's Free Wi-Fi Help Police Watch You?" *The Atlantic* (Apr. 2016), http://www.theatlantic.com/technology/archive/2016/04/linknyc-new-york-wifi-privacy-security/477696/.
28. Ibid.
29. The FCC proposes that services cannot be made conditional on opting in to data sharing, though these free services may (oddly) not qualify as common carrier BIAS providers because they are not offering telecommunications for a "fee." Note the "coffee shop" WiFi exemption to BIAS regulations is based on access provided to a particular *venue*, not broad areas of publicly-accessible space.
30. *See* Kevin Fagan et al., "New List of Water Hogs Includes Bankers, Lawyers, Former Warrior," *SF Gate,* October 29, 2015, http://www.sfgate.com/science/article/New-list-of-water-hogs-includes-bankers-lawyers-6598735.php.
31. For discussion of the "appliance load signatures" unique to every appliance, *see* Ariel Bleicher, "Privacy on the Smart Grid," *IEEE Spectrum,* October 5, 2010, http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid.
32. US Department of Energy, "DataGuard: Energy Data Privacy Program Voluntary Code of Conduct Final Concepts and Principles" (outline of voluntary best practices for smart grid data sharing, Washington, D.C., 2015) *available at* https://www.smartgrid.gov/files/DataGuard_VCC_Concepts_and_Principles_2015_01_08_FINAL.pdf.
33. Ibid.
34. *See* "TRUSTed Smart Grid Certification Standards," TRUSTe, accessed August 11, 2016, https://www.truste.com/privacy-certification-standards/trusted-smart-grid/.
35. *See* Martin H. Bosworth, "Loyalty Cards: Reward or Threat?" *Consumer Affairs*, July 11, 2005, https://www.consumeraffairs.com/news04/2005/loyalty_cards.html.

36. This is a poor benchmark for broadband competition. Even at 10 Mbps the number of competitors in a given market jumps considerably. *See* Robert D. Atkinson, "Wheeler Sets the Broadband Bar Higher tan South Korea," *Innovation Files,* (January 2015), http://www.innovationfiles.org/wheeler-sets-the-broadband-bar-higher-than-south-korea/.
37. Eric Null, Comcast Wants You to Empty Your Wallets to Protect your Privacy, *supra* note 24
38. Ibid.

ABOUT THE AUTHOR

Doug Brake is a telecommunications policy analyst at ITIF. He specializes in broadband policy, wireless enforcement, and spectrum-sharing mechanisms. He previously served as a research assistant at the Silicon Flatirons Center at the University of Colorado. Brake holds a law degree from the University of Colorado Law School and a bachelor's degree in English literature and philosophy from Macalester College.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.