Broadband Privacy: The Folly of Sector-Specific Regulation

BY DOUG BRAKE, DANIEL CASTRO, AND ALAN MCQUINN | MARCH 2016

Deviating from the historical harms-based privacy approach of the FTC framework would significantly disrupt ongoing dynamic competition in innovative new data uses, ultimately reducing deployment and adoption.

Emboldened by recent pressure from "broadband populists" and enabled by its ill-advised classification of broadband as a common carrier service under Title II of the Communications Act, the Federal Communications Commission (FCC) is considering the unprecedented step of regulating broadband privacy. Such regulations would be a mistake. The calls for rigid, paternalistic regulation from advocacy groups like Public Knowledge and New America Foundation are flawed; they systematically ignore the benefits of data innovation, downplay the advantages of industry best practices and the flexible Federal Trade Commission (FTC) framework, overstate risks, and understate customers' control over their privacy. Moreover, regulating ISP privacy under Title II would result in the opposite of the FCC's stated goals under Section 706—less broadband deployment and adoption.

Deviating from the historical privacy protections of the Federal Trade Commission (FTC) framework would significantly disrupt ongoing dynamic competition in innovative new uses of Internet data, ultimately slowing the rate of growth of broadband deployment and adoption and also degrading the online experience. Yet broadband populists hope to do just that, not in the name of protecting privacy as they claim, but as yet another tactic in their overarching strategy to turn the broadband industry into a heavily-regulated utility like gas or water, or, better yet, make the government be the sole provider of broadband services. Asymmetric regulation to cut off potential revenue streams that could be reinvested in networks or help lower prices is just one more tactic in their broader strategic fight to shrink private-sector broadband. Also pushing for expansion of rules are the privacy

activists, who see an FCC rulemaking as an opportunity to maneuver around Congress, and take a tactical step towards their endgame of a European-style privacy regime for the United States. Rather than pursue heavy-handed privacy rules and expand the scope of its utility-style regulation, the FCC should leave broadband privacy up the FTC and refocus on its core mission: supporting the expansion and advancement of America's communications networks.

BACKGROUND

In March 2015, the FCC carried out a sweeping policy change by reclassifying broadband Internet access service from an information service to a telecommunications service regulated under Title II of the Communications Act, even though it had access to less onerous means of regulating net neutrality. This shift in classification has wide-ranging implications in numerous areas of broadband policy.[1]

While initially forbearing from the legacy telephone regulations for which this law was intended, the FCC identified broadband privacy as one of its next priorities under its new Title II regime.[2] Referencing section 222 of the Communications Act, the FCC asserts new privacy powers arising from customer proprietary network information (CPNI) rules. While CPNI rules were originally intended to address information regarding basic landline telephone networks—such as phone numbers, consumers' history of purchases, and the frequency, duration, and timing of calls—the FCC now appears intent on a far broader reading of data subsumed by CPNI regulations, both in the telephone and broadband context.[3]

Not surprisingly, various broadband populist and privacy-focused organizations have vocally supported strong new rules. The New America's Open Technology Institute released a paper in January 2016, arguing that the FCC's decision to classify Internet access as a common carriage service allows it to use new tools to regulate Internet Service Providers' (ISP) privacy policies.[4] NAF went on to argue that ISPs have unique access to their subscribers' data, and because of this, the FCC should use this newfound power to create strong privacy rules for broadband Internet service. That same month, 59 organizations—many of which are on record as supporting government or local cooperative provision of broadband service—sent the FCC a letter urging the commission to start a rulemaking proceeding to develop privacy rules for broadband consumers.[5]

Privacy activists see this as an opportunity to make an end-run around Congress, where they have been unable to get any traction. They see ISP privacy regulations as a convenient foothold, which they hope to leverage into broader rules across the rest of the Internet, with the ultimate goal of a European-like precautionary-style privacy regime. Harold Feld of Public Knowledge has been quite candid on this strategy. On releasing a whitepaper that attempted to blur the jurisdictional lines between the FTC and the FCC, Feld explained, "you start with the broadband providers where you have a specialized agency with authority… That makes it a hell of a lot easier for the FTC…" in working on privacy problems with respect to edge providers.[6] This sort of privacy "leveling-up," whereby activists leverage sector-specific rules from the FCC across the entire ecosystem, should be avoided: as jurisdictional boundaries blur and start to overlap, innovation will be slowed

not just in broadband service, but throughout edge providers as well. The United States will then suffer the same damage to its Internet ecosystem as Europe.[7]

This sudden outpouring of feigned concern over broadband privacy is odd to say the least, as Americans have been subscribing to broadband for at least 15 years; until the FCC regulated it under Title II there was no hue and cry to regulate ISP privacy under a separate regime. There were no documented cases of consumer harm. It was only after the advocates had won their first battle in their war against ISPs—Title II classification—that they moved on to this next campaign.

There are many causes for concern with application of CPNI rules to broadband networks.[8] Most importantly, limiting the use of broadband data—which is qualitatively and quantitatively different from the CPNI imagined by the statute—would constrain broadband providers' ability to provide numerous benefits to consumers. Analyzing data is essential for ISPs to understand patterns and trends in Internet traffic and allows for informed adjustments to network functions and capacity, both in the long and the short term. Customer data is also important to help diagnose problems within the network and facilitate responses to customer requests for assistance with various issues.[9] The most efficient economic structure of these management functions—what costs to internalize, and where it would be better to rely on specialized third-parties—is not yet clear. Second guessing each such decision, running basic business choices through regulatory compliance, and analyzing the risk of running afoul of an unpredictable enforcement bureau, rapidly grinds innovation to a halt.

If the FCC applies privacy regulations above and beyond the existing FTC protections preventing unfair or deceptive practices, we would likely see less broadband deployment and adoption.

Moreover, there are numerous other opportunities for innovation using this type of data, most notably around targeted advertising, which can lower costs for consumers, increase revenues to pay for network upgrades, and make the economy overall more efficient.[10] To the extent customer data can be used for targeted advertising, provided customers have the ability to opt out (as shown below they now do) this should be celebrated, not feared. FCC regulations would unduly restrain business model flexibility and ISP pricing strategy, preventing internet service providers from offering discounts to the Americans who most need them in order to get online. Finally, if the FCC treats broadband providers as fundamentally different from other Internet actors, it would disrupt a nascent area of competition in the Internet ecosystem; government would be putting its thumb on the scale. But as noted above, for the broadband populists that is the whole idea--to get the government to turn private-sector ISPs into "losers," justifying additional regulatory encroachment.

Last May, the FCC issued a vague enforcement advisory, noting simply that broadband providers must take reasonable, good-faith steps to protect consumer privacy during the period between the effective date of the *Open Internet Order* and "any subsequent Commission action" applying Section 222 more specifically to broadband providers.[11] In truth, many in Washington expected the FCC to provide clarity in this space sooner, with Chairman Wheeler indicating proposed rules would be out last fall. Despite the fact that this has left operators with little guidance and great uncertainty, the FCC should not be faulted for this delay, as the Commission likely recognizes these issues are much more

complex than the various activists make them appear, and realizes the risk of inappropriately disrupting "competition, competition, competition" in broadband data innovation.

FCC PRIVACY REGULATIONS WOULD REDUCE THE RATE OF BROADBAND DEPLOYMENT AND ADOPTION

Put simply, if the FCC applies privacy regulations above and beyond the existing FTC protections preventing unfair or deceptive practices, we would likely see less broadband deployment and adoption.

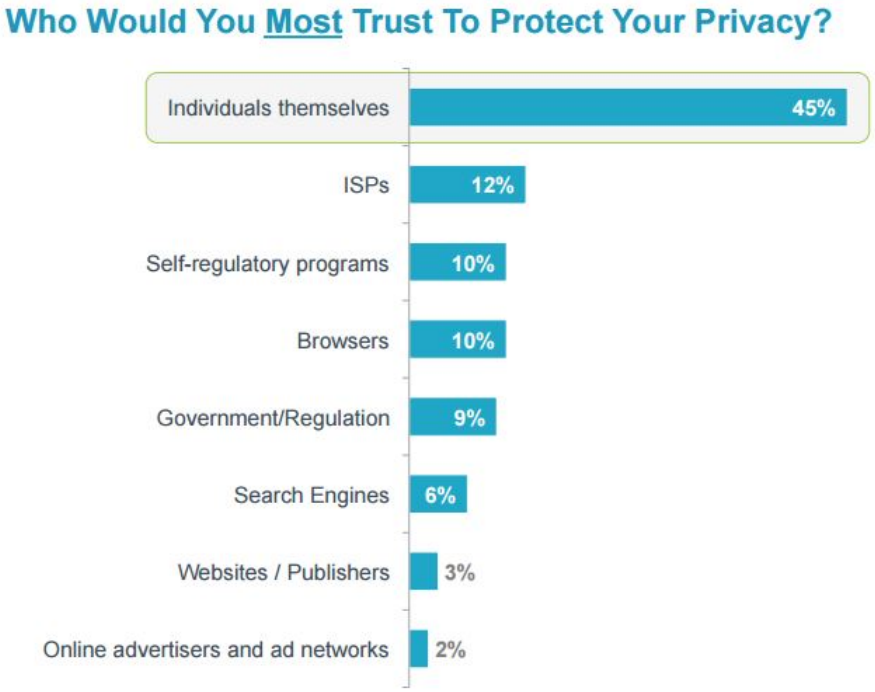
The Commission likely recognizes privacy issues are more complex than advocates want them appear, and realizes there is great risk of inappropriately disrupting "competition, competition, competition" in broadband data innovation.

But in order to justify its proposed action the FCC has developed an argument that asserts exactly the opposite. The Open Internet Order asserted that "consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth."[12] However, if you follow the Commission's footnotes, and examine the evidence the FCC cites, there is remarkably little, if any, empirical support for this assertion. Beyond more general worries about cybersecurity, there appears to be virtually zero support for the idea that privacy concerns about ISPs in particular harm the so-called "virtuous cycle," where demand for online services supposedly drives additional broadband deployment.

For example, in support of its section 706-based "virtuous cycle" privacy arguments, the FCC points to the NTIA's 2014 Digital Nation report, which plainly states "only 1 percent of household expressed privacy concerns . . . as their primary reason for not using the Internet at home."[13] The Pew Internet and American Society surveys of Americans' use of broadband yielded similar results. When non-adopters were asked why they don't own a smart phone, less than 1 percent of those surveyed listed "worried about privacy/tracking" as a reason. When non-adopters were asked why they don't subscribe to broadband, privacy did not even make the cut of possible reasons.[14] Moreover, considering the broad information ecosystem involved in the Internet and the FCC's narrow jurisdiction over common carriers, no rules the FCC can concoct are likely to allay the concerns of the 1 percent of Americans who are most privacy sensitive.

The FCC also points to a 2011 survey performed by TRUSTe, which, although it did find consumers consider privacy important, in no way shows that privacy policies on the part of ISPs hinder broadband use. In fact, when asked which Internet entity consumers trust the most to protect their privacy, the survey showed that, after individuals themselves (users overwhelming believed they themselves were best suited to protect their own privacy), ISPs were the most trusted.[15]

Figure 1: Who do consumers trust most to protect privacy online. Source: TRUSTe 2011 survey.[16]



It is ironic that the FCC, in grasping for support for regulation of ISP privacy practices, points to a survey showing that when it comes to protecting privacy consumers trust ISPs *more* than government regulation (albeit only marginally). This clarifies that support for general privacy regulations in the name of the "virtuous circle" of broadband deployment is without any foundation; the justification for asymmetric regulation on ISPs is even thinner.

The FCC makes the same mistake broadband populists and privacy advocates do when considering the effect of privacy on Internet use: they focus only on the demand side and not the supply side. By reducing ISP ad revenues and thereby raising the price of broadband services, privacy regulations would harm the supply of broadband, limiting both network upgrades and adoption. Regulations would unduly constrain innovations around pricing practices and business models, such as where an ISP could offer a discount for customers who participate in a particular program, or potential services offerings supported by targeted advertising. One of the benefits of the FTC approach focused on avoiding consumer harm is that allows for rapid innovation without assuming a particular industry direction, while protecting consumers and incentivizing industry to responsibly develop best practices. Indeed, this is one of the key reasons why the United States leads Europe in the Internet (and in broadband), as European privacy rules have made it extremely difficult for Internet companies to make adequate returns to support ad-supported services.[17]

One intriguing possible innovation is where providers offer a discount for broadband service based on support through targeted advertising or other monetization of data. Some advocates seem to think these practices necessarily pernicious, with Public Knowledge calling for strict scrutiny of these practices (and potentially a ban), and

New America Foundation going a step further, asking the FCC to bar discounts based on data collection.[18]

Still others seem to think there is some sort of "implicit bargain" between operators and end users that somehow militates against changes in ISP business models. The thinking is that because ISPs have traditionally provided service for a monthly fee, unlike many advertising supported servicers that are offered for free on top of the Internet, this is how things should stay forever. This line of thinking flies in the face of the actual diversity of business models, both in Internet access and in applications, and seems based on the assumption that business models do not change in the face of technological innovation. How a service is now priced, whether free or subscription-based or whatever, tells us nothing about the how it should be priced in the future. There is no reason to think customers actually expect the Internet ecosystem to remain static in terms of business models, and even if there was an expectation it would be bad policy to set any expectations in stone.

The FCC, grasping for support of regulating ISP privacy practices, points to a survey that says when it comes to protecting privacy consumers trust ISPs more than government regulation.

An example to consider is the new LinkNYC service, which is transforming payphone booths into free gigabit WiFi kiosks around New York City.[19] The new service has been heralded as giving free, super-fast Internet access to the public, but looking at the privacy policy and the partner companies, it is clear that this offering is premised on data collection and targeted advertising.[20] It would obviously be wrong to outlaw such a service, but this is just what a presumption of against flexible broadband pricing would do. High speed broadband is expensive and difficult to deploy; we should allow for innovation to drive new, more affordable models of deployment as much as possible.

An automatic presumption against these new kinds of pricing practices is remarkably anti-consumer. To the extent broadband user data can be monetized, there is a significant opportunity to reduce the cost of broadband service and thus expand broadband adoption. Recent research indicates that the cost of service may play more of a role in broadband non-adoption than initially thought (as compared to questions of relevance or digital literacy).[21] The opportunity to offer variable pricing based on data collection policies is potentially a boon for those looking for a lower-cost option to either get online or move towards a faster speed connection. Advertising supported broadband or other platforms will drive further broadband adoption and use.

Yet the paternalistic attitudes of broadband populists and privacy advocates (who say that they know what is best for all consumers, including low-income consumers), runs counter to what Americans really want. For example, Pew found that "Nearly half (47%) say the basic bargain offered by retail loyalty cards, which allow stores to track their purchases in exchange for occasional discounts, is acceptable to them," with another 20 percent saying that it might be acceptable.[22] Privacy advocates would deny two-thirds of Americans the right to choose, because they believe they know individual interests better than individuals do. Of course what the populists don't say is that what they want is for ISPs to give everyone the discount, whether they opt in or opt out of data collection and targeted ads. In their world, lower prices would not come from more ad revenue to ISPs, but from what they mistakenly see as excess ISP profits.[23]

Also, where operators are willing to put different price points on their data collection policies, the value of this data becomes apparent. Monetization of this data can offer operators a new revenue stream that can be reinvested in the network. Given appropriate privacy policies—which as we note below all the major ISPs have—these types of practices can drive broadband network upgrades. Undoubtedly the virtuous cycle pushes in the direction of additional experimentation in this area—not regulatory curtailment.

Telecommunications carriers are facing an expanding opportunity, especially with new capabilities enabled by recent technological developments in networking, to eventually offer personalized services to individual consumers at scale. While technologies such as software defined networking and network functions virtualization are still relatively new, the potential consumer value they can unlock is huge. But the lifeblood of personalized digital services is data. However well-intentioned the Commission is in wanting to protect user privacy, the rigidity of up-front regulations—as opposed to a more FTC harms-based approach—will slow new services that depend on data. Indeed, big data is currently transforming many areas of industry, and telecommunications is no different.

However, given their more general ideological antipathy towards private competition in the provision of broadband networks, broadband populists would sour at such a result, even if it would leave Americans better off, simply because it gives private broadband companies a better ability to do business. For these advocates, seeing strict privacy rules implemented over broadband companies is the next tactic in a broader strategy to cut off potential revenue streams from ISPs and further leverage their Title II win to clamp down on these businesses, transforming them into highly-regulated utilities.

ISPS ALREADY PROVIDE CONSUMERS MEANINGFUL CONTROL OVER THEIR PRIVACY

New America asserts that broadband providers have set up a false choice for consumers—that between the ability to connect to the Internet and consumer privacy.[24] This dichotomy is patently false. Current privacy policies of broadband providers already allow consumers to not only identify what type of data their ISPs collect and for what purpose it is collected, but allow users to control whether that information is used.

All five of the top broadband providers—Time Warner, Charter, Comcast, Century Link, Verizon, and AT&T—list what types of data they gather are "personally identifiable information" and what is CPNI, distinguishing between these types and aggregated or anonymous data. Each of their privacy policies also call describe why the information is collected. Most importantly, each privacy policy allows subscribers to opt out of 3rd party online advertising, and almost every policy explicitly states that users have the ability to opt out of all personal information and CPNI associated marketing.

Figure 2: Consumer protections located in the privacy policies of five top broadband providers.[25]

Privacy Policy Provisions	Comcast	AT&T	Time Warner Cable	Verizon	Century Link	Charter
Number of Subscribers[26]	23 million	16 million	13 million	9 million	6 million	5 million
Lists types of PII	Yes	Yes	Yes	Yes	Yes	Yes
Explains why data is collected	Yes	Yes	Yes	Yes	Yes	Yes
Ability to Opt-Out of CPNI Marketing	Yes	Yes	Yes	Yes	Yes	Yes
Explains How Data is Used in Marketing	Limited info, de-identified, anonymous, aggregated	Aggregate anonymous Personal info used for 1st party ads	Basic info, 3rd party available info, anonymous, aggregated	De-identified, Anonymous, aggregated	De-identified info, Use of cookies	Basic Info,3rd party available info, anonymous
Ability to Opt-Out of 3rd Party Ads	Yes	Yes	Yes	Yes	Yes	Yes
Lists when CPNI can be given to government	Yes	Yes	Yes	Yes	Yes	Yes
Describes Duration of Data Retention	Yes	Yes	Yes	Yes	Yes	Yes
Access to Personal Information Records	Upon online or written request	Upon online or written request	Upon written request	Upon online or written request	Upon online or written request	Upon written request

Current privacy policies of broadband providers already allow consumers to not only identify what type of data their ISPs collect and for what purpose it is collected, but allow users to control whether that information is used.

PRIVACY-ENHANCING TECHNOLOGIES PROVIDE FURTHER USER CONTROL

Broadband populists and privacy advocates called for new rules because they claim ISPs have a "uniquely detailed and comprehensive view of all of subscribers' unencrypted online communications, personal habits, and daily lives."[27] Similarly, the recent letter to the FCC from various groups asserted that there was no way for "consumers to avoid data collection by the entities that provide Internet access service."[28] Privacy advocates claim that ISPs

handle all of a user's Internet traffic, and subscribers have no choice but to share this information if they want to access the Internet. This is simply untrue.

ISPs do not have nearly the visibility critics suggest. First, as the cost of processing has continued to drop, the number of online services and sites that use encryption has dramatically increased. As a result, ISPs will have less and less insight into customers' Internet usage. Second, any customers who have a heightened sensitivity to privacy concerns are able use tools like Virtual Private Networks (VPN) or even onion routing to obscure online communications. Third, ISPs only have a partial view of subscriber online behavior since most use multiple devices and service providers.[29]

Use of Encryption

When subscribers use encrypted protocols with their browsers, such as the Secure Sockets Layer (SSL) or Hypertext Transfer Protocol Secure (HTTPS), the broadband provider is unable to access the content or information about the detailed links that the user visits. The only information the ISP is able to see is the metadata—data that describes information about the connection (e.g., the name of the website domain and the total volume of data transferred).

Given the tools for users to protect their privacy and the fact ISPs provide consumers with notice and control over the use of their data, there is no specific harm in the broadband marketplace that the FCC needs to correct.

As the cost of encrypting data has fallen, more websites have started to encrypt all traffic so that a third party cannot intercept exchanged information. As of April 2015, 29 percent of all Internet traffic in North America was encrypted, and that number is steadily rising.[30] This rate of adoption has been augmented by prominent players in the web ecosystem supporting encryption. For example, in 2014, Google started giving secure websites a small benefit in its search ranking algorithm and it has suggested it will weight this factor more in the future.[31] Similarly, the "Let's Encrypt" program is a free, automated encryption service designed to encourage more websites to adopt secure Internet protocols.[32] The on-demand media provider Netflix—which by April 2015 accounted for 35.7 percent of all bandwidth consumed by North American web users daily—has also promised to adopt HTTPS sometime in 2016.[33] This trend towards encryption that will continue to play out over time.

Use of VPNs

In addition to the increased prevalence of encrypted traffic, consumers also have the option to use VPNs, remote networks that users can connect to in order to securely browse the Internet. If a broadband subscriber is using a VPN, the ISP can see only that the subscriber accessed that VPN, not traffic information. If consumers feel there is value in using VPNs to obfuscate their online habits from ISPs, they certainly can take that option. Consider how users who have disliked the types of advertisements they were seeing online have adopted ad blocking technology. In fact, as of the second quarter of 2015, there were 45 million users running ad blocking software in the United States.[34] The fact that there is not a similar movement for adopting VPNs suggests that subscribers are not as concerned about the privacy of their data as some suggest.

Multiple Service Providers

To be sure, broadband providers could use their subscribers' information to create personalized services. Even considering the growing use of encryption, where users forego a VPN, broadband providers will be able to identify certain characteristics of their users based on metadata and other online tracking technologies, just as other actors in the Internet ecosystem can. However, this data is far less complete than advocates describe. For example, the New America report says, "By monitoring the requests that their DNS servers receive, ISPs can easily build a comprehensive list of every domain name that each subscriber looks up—which is equivalent to knowing every website and service that the subscriber visits or uses."[35] This does not take into account that many consumers subscribe to multiple ISPs for service. As of July 2015, 55 percent of U.S. adults report having both a smartphone and a home broadband subscription.[36] These adults may also connect periodically to the over 9 million Wi-Fi hotspots spread throughout the United States.[37] Furthermore, many households have multiple devices and ISPs do not always have the ability to link across devices. Therefore, each individual broadband provider sees only a portion of a user's online activity rather than the comprehensive view that some advocates have described. And most of these customers use the same browser, search engines, social media platforms, and e-commerce sites across devices and service providers.

Given the advent of tools for users to protect their privacy and the fact ISPs provide consumers with meaningful control over the use of their data, there is no specific consumer harm in the broadband marketplace that the FCC needs to correct. Broadband providers already give users privacy controls by offering the explicit ability to opt out of data use. If a broadband provider states that it will allow consumers to opt out of these data-driven services, and that provider does not follow that practice, then it would be subject to the FTC unfair and deceptive acts enforcement.[38]

THE FCC'S GOAL SHOULD BE TO MINIMIZE COSTS AND ENCOURAGE INNOVATION

Asymmetric regulation would disrupt ongoing competition and industry dynamics related to Internet data. Presently, web tracking is diverse, competitive, and overseen by several regulatory regimes. Treating broadband providers as fundamentally different from other online actors would harm, not help the Internet ecosystem. Instead, a common regime, following in the foot-steps of FTC's oversight of a self-regulated industry, would allow for innovation across different sectors and not tip the scale in the direction of any particular Internet industry segment.

As the FCC weighs privacy rules for broadband providers it should not treat ISPs differently than other similarly situated online entities, such as search engines, social networks, e-commerce websites, operating systems, and others. Each of these Internet actors share much in common with broadband providers, using data to improve customer experience, improve advertising efficiency, and gain other benefits for consumers and the economy. Each has relatively similar access to its users' data; ISPs can see a similar type and amount of data as other actors in the ecosystem.

Moreover, online advertising is largely overseen by enforceable self-regulatory regimes. In December 2007, the FTC released a proposed set of rules for industry self-regulation, and in response the Digital Advertising Alliance (DAA) created its own principles for the industry.[39] In May 2011, the DAA, Better Business Bureau, and the Direct Marketing Association partnered to develop an enforcement program for compliance to this self-regulatory program.[40] Today, the FTC can hold these businesses accountable for their stated advertising practices by penalizing infringing companies.[41] Similarly, the privacy policies of operating systems like Apple's OS X and Google Android are also subject to FTC enforcement if they misrepresent how they use their users' personally-identifiable information. This is the model for a well-functioning, self-regulatory environment that maintains the flexibility needed for rapid innovation and experimentation with welfare-enhancing business models. Broadband providers should not face steeper burdens for implementing advertising than already exist.

The overwhelmingly superior policy choice is to continue with the framework that governed broadband privacy prior to the FCC's decision to classify broadband as a common carrier service.

History cautions against technology-specific rules that could create different frameworks for industry regulation. Instead of attempting to shape future technology trends through a regulatory framework, the FCC should rather encourage innovative models that decrease costs and improve services for consumers. It should avoid responses that affect how broadband providers price their products. Many companies are trying to figure out what value consumers place on privacy-sensitive services, and what experimentation the market will accept. This process should focus not only on broadband Internet but also on other sectors under the FCC's jurisdiction, like cable TV. Innovation-friendly rules would allow providers to experiment with business models, including customized television advertisements based on user data. The FCC should encourage this type of data use—not attempt to curtail or control it.

Broadband providers are not the only direct beneficiaries of this data, as some privacy advocates argue—even if they were, that benefit translates into more investment. In fact, consumers can get direct benefits through lower priced and more customized offerings, and society in general benefits from greater levels of efficiency in advertising with less money spent on poorly targeted ads. This has led to services like AT&T's Gigapower, which offers a $29 per month discount for consumers who allow AT&T to use their data for targeted advertisements.[42] Others are experimenting with additional services, such as mobile video, on ad-supported platforms.

Considering the above trends in technology and the potential for innovation to drive welfare-advancing benefits in this area, the following recommendations should guide the FCC going forward.

First and foremost, the Commission should leave ISP privacy to the FTC.

As explained above, the overwhelmingly superior policy choice is to stick with the framework that governed broadband privacy prior to the FCC's decision to classify broadband as a common carrier service (which ITIF argued against at the time). The Commission may worry that it is constrained by the legalistic trap set by activists, who wrongly claim the FCC is bound by statute to regulate privacy.[43] But, in addition to its

forbearance powers, the FCC has a great deal of power to interpret the statute, and should do so based on the best policy.

Splintering off sector-specific rules would create a troubling problem as a wide variety of government agencies attempt to control their historical regulatory jurisdiction in an age of technological convergence. This problem is likely to be exacerbated as information technology is integrated more tightly with additional verticals through advances such as the Internet of Things. Consistently applied innovation-friendly policies across the entire Internet ecosystem should be the preferred policy, and there are a number of routes to achieve this.

The cleanest legal solution to achieve this policy goal is for the FCC to recognize that ISP privacy practices are non-common carrier activities, and thus the FTC is not precluded from acting with regard to broadband privacy.[44] The FCC should then forebear from section 222 of the Communications Act entirely, and clarify the existing memorandum of understanding between the two agencies that broadband privacy is the province of the FTC.

If the FCC unwisely decides it necessary to pursue privacy regulations for broadband access providers, the FCC should take a very narrow reading of the statute and aim to keep its rules as consistent with FTC practice as possible.[45]

Any path forward should maintain a light-touch approach consistent with other parts of the Internet ecosystem. As discussed above, there is nothing about broadband providers' particular access to data that justifies differing rules, especially when data are now by-and-large a commodity. Therefore, if the FCC does pursue a rulemaking, regulations should aim for a harms-based, FTC-like approach as much as possible. Holding carriers to their stated policies and best practices has the consistency that allows for dynamic competition across industries and the flexibility that fosters innovation.

Second, the FCC should encourage the continued formation of industry best practices.

Transparency, notice, and choice do much of the heavy lifting in this area, helping inform customers and allowing ISPs to retain consumer trust. The truth is that while privacy is an important value, it must be balanced with other goals, such as cost, enhanced functionalities, and usability. Furthermore, broadband users are not uniform in their privacy preferences. Some users would happily give up personal information for lower priced services, while others go to great lengths to remain anonymous, even if it means paying more. A dynamic back-and-forth between industry, users, and civic society is better suited to explore the proper balance of interests than rigid regulations.

Consider the case of Verizon's so-called "super-cookie." In October 2014, news stories described a practice by Verizon Wireless of modifying some of its cellular web traffic to insert a Unique Identifier Header (UIDH), dubbed a "super-cookie," that helped create profiles for targeted ads.[46] Listening to the concerns of the privacy community, Verizon voluntarily changed its policy in March 2015, and began allowing users to opt out of the tracking program.[47]

This clearly shows that ISPs are indeed informed and guided by public reaction to these practices. Some advocates attempt to paint this as an area where ISPs are unconstrained, which simply is not true. By promoting a dynamic process whereby consumers can inform the particular shape of privacy consent processes, in combination with existing "opt out" possibilities, concerns around ISP data collection disappear. Consumers that object to a broadband provider's CPNI policy would not have to switch carriers if they can simply opt out.

Third, the FCC should support ISP experiments with pricing around innovative uses of consumer data.

Customers place differing values on their privacy. It is not the role of the FCC or government generally to deprive consumers of these choices, especially those that may help increase access for low-income populations. Furthermore, to exclude these options would be antithetical to the commission's goal of providing universal access to broadband for all Americans and driving the virtuous cycle of Internet growth.

Fourth, the FCC should encourage carriers to use, disclose, and permit access to aggregated and de-identified customer information.

Customer network data has important uses that benefit consumers, such as improving network performance, fostering personalized digital services, and potentially improving efficiency throughout a number of verticals, like healthcare or insurance.[48] As ITIF and the former privacy commissioner of Ontario have shown, when data is properly de-identified, the potential risks of re-identification is low.[49] ISPs should be encouraged to use aggregated or de-identified data since it has many beneficial uses with little potential for consumer harm.

Finally, the FCC should rely on the FTC to bring enforcement actions if they find that consumers face specific privacy harms or broadband providers intentionally violated their stated privacy policies.

The enforcement process in the case of misuse of consumer data should be clear and straightforward. Clear rules will make the enforcement process easier and allow for more rapid experimentation in beneficial uses of broadband data. Fines should be reasonably tied to actual consumer harm and amplified when the action that caused the harm was intended.[50] This will allow the commission to place value on appropriate uses of the information and avoid imposing liability for technical violations that did not cause consumer harm.

CONCLUSION

As the FCC weighs enacting privacy regulations for broadband Internet access services, it risks crafting a solution in search of a problem—in fact, a solution that would create a problem. Regulations would reduce the efficiency of the broadband industry, with resultant loss of broadband network investment and higher prices for broadband consumers. These are precisely the goals of broadband populists pressuring the FCC to act. For the rest of us, these are results we should avoid, for they would retard, not advance the important goal of universal broadband deployment and adoption.

ENDNOTES

1. See "Hearing on The Uncertain Future of the Internet, Before the House Energy & Commerce Subcommittee on Communications and Technology," 114th Cong. (2015) (testimony of Robert D. Atkinson, Founder and President, Information Technology and Innovation Foundation) available at http://energycommerce.house.gov/hearing/the-uncertain-future-of-the-internet.
2. See Mario Trujillo, "FCC to Tackle Broadband Privacy in 'Next Several Months,'" *The Hill*, Nov. 5, 2015, http://thehill.com/policy/technology/259232-fcc-to-tackle-broadband-privacy-in-next-several-months (quoting Chairman Wheeler during an interview with Charlie Rose).
3. FCC Enforcement Bureau Chief Travis LeBlanc has commented that 47 U.S.C. § 222(a) references a duty to protect "propriety information," which, to his interpretation, gives the FCC authority over a much broader set of data than CPNI as historically understood. See also, Joseph Jerome, Travis LeBlanc on the FCC's New Privacy Role, *Future of Privacy Forum*, Dec. 11, 2014 https://fpf.org/2014/12/11/travis-leblanc-on-the-fccs-new-privacy-role/.
4. "The FCC's Role in Protecting Online Privacy," *New America*, January 2016, https://static.newamerica.org/attachments/12325-the-fccs-role-in-protecting-online-privacy/CPNI__web.d4fbdb12e83f4adc89f37ebffa3e6075.pdf.
5. For example, Access Humbolt promotes "free speech and community media - by the people; for the people," and does not appear to have a stated privacy policy. Access Humbolt, "Local Voices Through Community Media," accessed Feb. 25, 2016, http://accesshumboldt.net/site/; U.S. PIRG's position is that Locally owned and operated networks support these familiar core goals of communications policy, and therefore should receive priority in terms of federal and state support. U.S. PIRG, "A Public Interest Internet Agenda," Sept. 21, 2009, http://uspirg.org/reports/usp/public-interest-internet-agenda; The Center for Rural Strategies states with regard to broadband, "Local ownership and investment in community are priorities." *Center for Rural Strategies,* accessed Feb. 25, 2016, http://www.ruralstrategies.org/broadband; Access et al., "Broadband Privacy Rulemaking," *New America*, January 20, 2016, https://static.newamerica.org/attachments/12311-oti-joins-coalition-calling-for-greater-protection-of-online-privacy-for-broadband-consumers/Broadband_Privacy_Letter_to_FCC.ab06f1ece7fa4d3c98f33b75910287fb.pdf.
6. Harold Feld, remarks at "Preserving Broadband Network Privacy," February 17, 2016, The U.S. Capitol Visitor Center, https://www.publicknowledge.org/events/preserving-broadband-network-privacy.
7. *See, e.g.*, Avi Goldfarb & Catherine E. Tucker, Online Advertising, Behavioral Targeting, and Privacy, *Communications of the ACM*, vol 54, May 2011, http://www.cs.grinnell.edu/~davisjan/csc/105/2012S/articles/CACM-privacy.pdf.
8. Although overlooked in the broader policy debate, some challenges of applying section 222 to broadband are quite basic, such as what type of information would even count as CPNI, especially when very little data is available "solely by virtue of the carrier-customer relationship," as required by the statute. 47 U.S.C. § 222 (h)(1)(A).
9. Doug Brake, Daniel Castro, and Robert Atkinson, "The FCC's Privacy Foray: Privacy Regulations Under Title II," *Information Technology and Innovation Foundation*, April 2015, http://www2.itif.org/2015-fcc-privacy.pdf?_ga=1.87452753.812486504.1449157248.
10. See, e.g. Daniel Castro, "Stricter Privacy Regulations for Online Advertising Will Harm the Free Internet," *Information Technology and Innovation Foundation*, September 2010, http://www.itif.org/publications/stricter-privacy-regulations-online-advertising-will-harm-free-internet.
11. Federal Communications Commission, FCC Enforcement Advisory, Public Notice, DA 15-603, May 20, 2015, https://apps.fcc.gov/edocs_public/attachmatch/DA-15-603A1.pdf.
12. Federal Communications Commission, In the Matter of Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, FCC-15-24, Feb. 26, 2015, ("Open Internet Order"), paragraph 54.
13. Open Internet Order at paragraph 464, citing the 2015 Broadband Progress Report at paragraph 104, citing, 2014 NTIA Digital Nation Report.
14 John B. Horrigan & Maeve Duggan, "Home Broadband 2015," *Pew Research Center*, Dec. 21, 2015, http://www.pewinternet.org/files/2015/12/Broadband-adoption-full.pdf p. 15
15. Open Internet Order at 54, citing TRUSTe and Harris Interactive, "2011 Consumer Research Results Privacy and Online Behavioral Advertising," July 25, 2011, ("TRUSTe survey") *available at*

https://web.archive.org/web/20120227094350/http://www.truste.com/ad-privacy/TRUSTe-2011-Consumer-Behavioral-Advertising-Survey-Results.pdf.

16. TRUSTe survey at 13.
17. Richard Bennett, et. al, *The Whole Picture: Where America's Broadband Networks Really Stand*, Feb. 2013, http://www2.itif.org/2013-whole-picture-america-broadband-networks.pdf; Guillaume Xavier-Bender, ed. "Seeing the Forest for the Trees: Why the Digital Single Market Matters for Transatlantic Relations," The German Marshall Fund of the United States, page 8.
18. "The FCC's Role in Protecting Online Privacy," *New America* at 8.
19. *See*, Michael Grothaus, "New York City Officially Launches Free Public WiFi," Fast Company, Feb. 18, 2016, http://www.fastcompany.com/3056861/fast-feed/new-york-city-officially-launches-free-public-wi-fi.
20. CityBridge, LLC, "CityBridge Privacy Policy," Nov. 2014, http://www.nyc.gov/html/doitt/downloads/pdf/Proposed-PCS-Franchise-Exhibit-2-CityBridge-Privacy-Policy.pdf.
21. *See, e.g.* Amina Fazlullah, "Research Shows Cost is Biggest Barier to Broadband Adoption," Benton Foundation, Jan. 11, 2016, https://www.benton.org/blog/research-shows-cost-biggest-barrier-broadband-adoption.
22. Lee Rainie & Maeve Duggan, "Privacy and Information Sharing," Pew Research Center, Jan. 14, 2016, http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.
23. As ITIF showed in The Whole Picture, U.S. ISP profit rates are actually lower than European. *See* The Whole Picture, *supra* note15.
24. Emily Hong, "Privacy Vs. Connectivity: A False Choice," *New America*, February 1, 2016, https://www.newamerica.org/oti/privacy-vs-connectivity-a-false-choice/.
25. Time Warner Cable Subscriber Privacy Notice, Time Warner Cable, https://help.twcable.com/twc_privacy_notice.html; Charter Commercial Subscriber Privacy Policy, Charter, https://www.charter.com/browse/content/commercialprivacy; Customer Privacy For Cable Video, High-Speed Internet, Phone, and Home Security Services, Comcast, http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html; Privacy Policy, Century Link, http://www.centurylink.com/Pages/AboutUs/Legal/PrivacyPolicy/; Privacy Policy, Verizon, http://www.verizon.com/about/privacy/full-privacy-policy; AT&T Privacy FAQ, AT&T, http://www.att.com/gen/privacy-policy?pid=13692.
26. Leichtman Research Group, Top Broadband Internet Providers in the U.S., Q42015. http://www.leichtmanresearch.com/research/notes12_2015.pdf
27. Harold Feld et. Al, "Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World," Public Knowledge, Feb. 2016, https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper(1).pdf; "The FCC's Role in Protecting Online Privacy," *New America.*
28. Access et al., "Broadband Privacy Rulemaking," *New America*, January 20, 2016, https://static.newamerica.org/attachments/12311-oti-joins-coalition-calling-for-greater-protection-of-online-privacy-for-broadband-consumers/Broadband_Privacy_Letter_to_FCC.ab06f1ece7fa4d3c98f33b75910287fb.pdf.
29. Peter Swire, Presentation at State of the Net, available at http://peterswire.net/wp-content/uploads/stateofthenet.012516.pptx.pdf.
30. "Global Internet Phenomena Spotlight Encrypted Internet Traffic," *Sandvine*, April 8, 2015, https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.
31. "HTTPS as a ranking signal," *Google*, August 6, 2014, https://googleonlinesecurity.blogspot.com/2014/08/https-as-ranking-signal_6.html.
32. "About" *Let's Encrypt*, February 12, 2016, https://letsencrypt.org/about/.
33. "Global Internet Phenomena Spotlight Encrypted Internet Traffic," *Sandvine;* Chris Welch, "Netflix will make browsing movies more secure within the next year," *The Verge*, April 15, 2015, http://www.theverge.com/2015/4/15/8422889/netflix-https-coming-within-one-year.
34. "The 2015 Ad Blocking Report," *PageFair*, 2015, https://blog.pagefair.com/2015/ad-blocking-report/.
35. "The FCC's Role in Protecting Online Privacy," *New America.*

36. John Horrigan and Maeve Duggan, "Home broadband adoption: Modest decline from 2013 to 2015," *Pew Research Center*, December 21, 2015, http://www.pewinternet.org/2015/12/21/1-home-broadband-adoption-modest-decline-from-2013-to-2015/.
37. Wi-Fi Growth Map, iPass, http://www.ipass.com/wifi-growth-map/.
38. 15 U.S. Code § 45 - Unfair methods of competition unlawful; prevention by Commission, https://www.law.cornell.edu/uscode/text/15/45
39. "Self-Regulatory Principles For Online Behavioral Advertising," *Federal Trade Commission*, February 2009, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-reportself-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.
40. "Digital Advertising Alliance Begins Enforcing Next Phase of Self-Regulatory Program for Online Behavioral Advertising," *Digital Advertising Alliance*, May 23, 2011, http://www.aboutads.info/resource/download/DAA_Compliance_FINAL.pdf
41. "FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network," *Federal Trade Commission*, March 30, 2011, http://www.ftc.gov/news-events/press-releases/2011/03/ftc-chargesdeceptive-privacy-practices-googles-rollout-its-buzz.
42. Jon Brodkin, "AT&T charges $29 more for gigabit fiber that doesn't watch your Web browsing," *Ars Technica*, February 16, 2015, http://arstechnica.com/business/2015/02/att-charges-29-more-for-gigabit-fiber-that-doesnt-watch-your-web-browsing/.
43. *See* Feld et. Al, "Protecting Privacy, Promoting Competition," *supra* note 26.
44. Generally speaking, the common carrier exemption in the FTC Act precludes the FTC from addressing common carrier practices, leaving these to the specialized regulator.
45. Note, from a legal perspective, what constitutes CPNI in the broadband context is likely quite narrow: the statute limits the heightened protections of CPNI to only information that is "made available to the carrier by the customer *solely by virtue of the carrier-customer relationship*" (emphasis added). 47 U.S.C. § 222(h)(1)(A). As most broadband data is freely transferred among players as packets pass from end to end of an Internet connection, information that is available solely by virtue of the carrier-customer relationship is far narrower than even what was considered CPNI in the telephone context.
46. Robert McMillan, "Verizon's 'Perma-Cookie' is a Privacy-Killing Machine," *Wired*, October 27, 2014, http://www.wired.com/2014/10/verizons-perma-cookie/.
47. Brian Chen, "Verizon Wireless Customers Can Now Opt Out of 'Supercookies'," *New York Times*, March 31, 2015, http://bits.blogs.nytimes.com/2015/03/31/verizon-wireless-customers-can-now-opt-out-of-supercookies.
48. For example, this data may be used to identify and improve real-time information about traffic patterns, thereby reducing congestion and enabling transportation planners to improve roadways or better deploy transit options.
49. Ann Cavoukian and Daniel Castro, "Big Data and Innovation, Setting the Record Straight: De-identification *Does* Work," June 16, 2014, http://www2.itif.org/2014-big-data-deidentification.pdf.
50. Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene," *Information Technology and Innovation Foundation*, February 2015, http://www2.itif.org/2015-how-whenregulators-intervene.pdf.

ABOUT THE AUTHORS

Doug Brake is a telecommunications policy analyst with the Information Technology and Innovation Foundation. 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. Doug holds a law degree from the University of Colorado Law School and a Bachelor's in English Literature and Philosophy from Macalester College.

Daniel Castro is the vice president of the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Alan McQuinn is a research assistant with the Information Technology and Innovation Foundation. Prior to joining ITIF, Mr. McQuinn was a telecommunications fellow for Congresswoman Anna Eshoo and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He got his B.S. in Political Communications and Public Relations from the University of Texas at Austin.

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.