The FCC's Privacy Foray: Privacy Regulation Under Title II

BY DOUG BRAKE, DANIEL CASTRO, AND ROBERT D. ATKINSON | APRIL 2015

It is important to recognize that broadband network data is fundamentally different than the customer information imagined in the Telecommunications Act of 1996.

The ill-advised classification of broadband as a Title II telecommunication service triggered a cascading series of additional proceedings to sort through the wide-ranging implications of this policy shift. Prominent among these issues that the FCC must now address is the treatment of customer proprietary network information (CPNI) by broadband access providers. In the workshops and proceedings to come, it will be important to recognize that broadband network data is fundamentally different than the CPNI imagined in the Telecommunications Act of 1996. The difference in the information, coupled with its increased functionality and value should encourage regulators to allow room for a flexible, voluntary framework atop baseline expectations of privacy. While many aspects of this issue remain to be explored, policymakers should prefer transparent and flexible "opt-out" mechanisms over a rigid liability regime. Doing so will enable more diverse, consumer friendly business models and help drive innovation.

INTRODUCTION AND BACKGROUND

In March 2015, the Federal Communications Commission (FCC) undertook a historic change in policy: classifying broadband Internet access service as a telecommunications service to be regulated under Title II of the Communications Act. While this dramatic

policy shift was purportedly necessary to implement net neutrality rules, the change in classification has wide-ranging implications for other areas of telecom policy.[1]

In the Open Internet Order, the commission identified a handful of the most glaring areas that will soon need to be addressed under a Title II regime, including customer privacy.[2] The customer privacy laws at issue here, found in section 222 of the Communications Act, are known as the customer proprietary network information (CPNI) rules.[3] Congress adopted these laws as part of the Telecommunications Act of 1996, and when the FCC first implemented these laws it focused primarily on competitive concerns instead of privacy.[4] Over the course of many proceedings, interpretation of the law has focused more and more on privacy.[5]

The CPNI rules have also grown beyond the plain old telephone service, now applying to information generated as part of interconnected VoIP and mobile voice service.[6] As part of the Open Internet Order, the commission has now expanded these rules to broadband providers as well.[7]

The CPNI rules have grown beyond the plain old telephone service and now apply to information generated as part of mobile voice and interconnected VoIP. As part of the Open Internet Order, the commission has now expanded this law to broadband providers as well.

CPNI and Legacy Networks

Generally speaking, section 222 governs telecommunications carriers' protection and use of information obtained from their customers or other carriers—but what information? The law defines CPNI as:

> *(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.*[8]

In the context of a landline telephone network, what this type of data was and where it was stored was relatively straightforward. Congress was concerned with "information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting."[9] What information is covered in the broadband context is a more difficult question. A broad reading of this definition would potentially sweep in a wide array of data such as network traffic and browsing history.

With regard to how telecommunications carriers treat this data, earlier interpretations of section 222 were quite strict. For example, because these laws were largely written as restrictions on incumbent local exchange carriers, the legacy interpretation for telephone networks greatly restricted the circumstances under which a carrier could use CPNI for marketing or to provide customized services. The rules required customer consent before carriers could use, disclose, or permit access to CPNI generally. These restrictions were accompanied by liability to protect this information, which the commission has characterized as mandating a duty of "the greatest level of protection."[10]

Public Knowledge, which lobbied the commission to apply CPNI laws to broadband,[11] has recognized the power of this law, stating that "these rules are no joke," and that "the strength and particularity of these rules are comparable to those of the HIPAA Rules" that cover medical records.[12]

While some CPNI is quite sensitive, such as billing information and social security numbers, much is not, such as monthly bandwidth usage. And certainly most CPNI is not as sensitive as medical records are. If CPNI includes browsing history, some information may be quite sensitive, but the important point is not all data has the same level of sensitivity, and, as a result, we need flexible rules.

Collection of most CPNI is perfectly legitimate as a normal part of a service. Beyond simple billing information, operators also use CPNI to diagnose problems within the network and assist in responding to customer requests for assistance with device, service, or performance issues.

Furthermore, as ITIF has long argued, much good can come from sharing and working with this kind of data, such as lower costs for consumers from targeted ads.[13] The commission should recognize that the functionality and value of broadband CPNI is much higher than the CPNI of legacy networks. Much more can be made through innovative uses of, say, aggregated location data than numbers on how many customers purchase call waiting. And it will be important to remember that this is not a zero-sum game, as many privacy advocates portray it to be, with carriers getting all the benefits of being able to use data and consumers getting none. 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.

Finally, unlike the days of plain old telephone service, broadband providers have much more in common with the broad range of Internet actors in the digital ecosystem (search engines, social networks, e-commerce websites, and the like) who all use data to improve customer experience, improve advertising efficiency, and gain a myriad of other benefits for consumers and the economy. Treating broadband providers as fundamentally different makes little sense and would harm, not help the Internet ecosystem.

This report sets aside several open questions to examine a potential path for FCC regulation of privacy on broadband networks. We momentarily abstain from questioning the wisdom of applying Title II in general, or section 222 in particular, to broadband networks. Likewise, we assume that the classification of broadband access service as a telecommunication service remains, and does not fall under legal challenge or administrative change. We also assume the FCC will retain jurisdiction over consumer privacy when it comes to information provided to telecommunications carriers generally, rather than allowing the Federal Trade Commission to continue its historical oversight of online privacy. In short, we assume the FCC moves forward unabated with CPNI rules for broadband providers and offer commentary on the general shape those rules should take.

FLEXIBLE DATA SHARING AND USE

Given the value and functionality of much of this information, broadband providers should have flexibility in utilizing it for their own purposes as well as sharing it with third parties, assuming these uses comport with baseline privacy rules that protect consumers.

Collection of most CPNI is perfectly legitimate as a normal part of a providing service. Beyond simple billing and identification information, operators can also use technical

CPNI to diagnose problems within the network and assist in responding to customer requests for assistance with device, service, or performance issues. The collection and use of this data is uncontroversial, even if important questions about the scope of CPNI rules and the liability for unauthorized sharing remain.[14]

Somewhat more controversial is the use of this data by broadband providers for marketing and providing customized services. And even more controversial is the sharing of some CPNI with third parties. The FCC should establish a basic framework for how this information should be used and shared, and it should allow industry and other stakeholders flexibility to generate best practices to extend that framework.[15]

Option for Consumers to Opt Out

A main component of a fundamental baseline of privacy should be allowing consumers the opportunity to choose not to have certain CPNI shared with third parties. Before sharing or using any information that could reasonably be used to identify an individual consumer, a carrier should have that consumer's consent, at least in the form of an ability to opt out.

This requirement for consent before disclosure is clearly required for telecommunications carriers by section 222.[16] However, the commission has retained considerable latitude in determining what constitutes consent.[17] Carriers should have flexibility in how they obtain consent for disclosure, and they should be able to satisfy the consumer disclosure consent rule by giving customers notice and an opportunity to opt out. As has historically been the case, implied consent should suffice for using as well as sharing most CPNI.[18]

Carriers may well choose not to share some types of information with certain third parties or to take further steps to obtain customer consent, but the commission should trust the granular decisions to evolving industry best practices instead of attempting to identify detailed rules for every possible sharing scenario.

Implied consent should likewise be required for a carrier's internal use of CPNI that is not necessary for provision of telecommunication services. For example, carriers may internalize functions for which data may otherwise be shared and deliver something to users based on use of CPNI, or they may perform some type of analytics on behalf of another client. The basic privacy framework should apply here as well.

Visible and Transparent

Processes around obtaining consent to share or use personally identifiable CPNI should be clear and straightforward for consumers to navigate. Data use and sharing practices should be fully transparent as well.

Some may argue that switching costs, market power, or even the wooly "gatekeeper" theory would make more onerous restrictions on telecommunication carrier use of CPNI necessary. But when carrier's consent processes are visible, transparent, and consumers have a clear, easy-to-navigate opportunity to opt out, these concerns vanish. Consumers would not have to switch carriers if they object to CPNI policy, but instead simply opt out. At the same time, these concerns justify the baseline implied consent requirement.

Flexibility around Pricing

There is real value in the innovative uses to which CPNI can be put, and consumers put different values on the release of their information. Some privacy advocates place an infinite value on their personal information. But policymakers should not let the preferences of a small group of vocal advocates trump the diverse needs of most American consumers. Many broadband customers would be more than happy to trade use of their personal information for a lower-priced or higher-quality broadband offering. It is not the role of the FCC or government generally to deprive consumers of these choices. Policymakers should allow carriers to experiment with pricing around CPNI policies.

We should not penalize those consumers who are willing to make the trade-off of their data in exchange for lower fees and avoid locking down specific business models, especially those that may help increase access for low-income populations. To exclude these options would be antithetical to the commission's goal of providing universal access to broadband for all Americans. There is real potential for carriers to leverage CPNI and other data for new, socially valuable purposes, and the commission should take care not to discourage existing carriers from experimenting with different business models or new entrants looking to explore possible synergies.

AGGREGATE AND DE-IDENTIFIED DATA

Under existing privacy rules, carriers are permitted to use, disclose, and permit access to CPNI that has been aggregated and de-identified. The FCC should ensure that if it does pursue rulemaking under section 222, then it will not impair the ability of carriers to use aggregated and de-identified data or undermine availability of this data to others. CPNI data may have important uses for consumers, especially as new opportunities are identified for using geo-location data. 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.

It has been clearly demonstrated that if employed properly, data de-identification techniques are effective in protecting privacy, and the potential upside to innovative uses of aggregate and de-identified data is immense.[19] Regulators should allow for the sharing of aggregate data and make clear that carriers will not face liability for sharing properly de-identified data.

SCOPE

Applying CPNI rules to broadband providers represents a large expansion of the FCC's jurisdiction over an important and growing sector of the economy. That authority should be limited as this area continues to develop. Similarly, the scope of potential liability should be clear and precise, with fines limited to situations with actual consumer harm or intentional violations, including negligence, of the security standards expected by regulators.[20]

Jurisdiction

The scope of information that should qualify as CPNI remains a difficult question. The FCC should exercise humility when considering how far into the Internet protocol stack its

jurisdiction now reaches for fear of chilling innovation in other parts of the vibrant U.S. innovation ecosystem.[21]

As a general matter, it makes little sense for telecommunications carriers to be subject to reporting requirements and liability for release of information that also can be easily gathered by others online. When, for example, Web tracking is commonly undertaken by numerous third parties and is already overseen by other regulatory bodies, telecom carriers should not face steeper burdens for implementing these types of services. Moreover, it is not yet clear which stakeholder in the Internet ecosystem is best positioned to deliver relevant ads to users, but telecom carriers may provide a more useful solution than others while better protecting the privacy of users. Indeed, the FCC should attempt to keep its policies in line with practices in other parts of the ecosystem.

Liability

The FCC should only consider enforcement actions if it finds that consumers face specific privacy harms or telecom carriers intentionally violate any required security practices. Beyond due process concerns, liability for unauthorized CPNI access should be clear for good policy reasons. Clarity in these rules is necessary to allow for experimentation in beneficial uses of CPNI. A liability regime that is either too strict or too vague could well stifle these uses.

This is a complex area of rapid technological development, with third parties often specializing in information gathering and analysis. The commission should consider the negative incentives its rules could create and take into account the potential to undermine the development of an efficient economic ecosystem in this area.

Furthermore, any fines should be reasonably tied to actual consumer harm and amplified when the action that causes that harm was intended.[22] The FCC should recognize the value in the appropriate use of this information, and impose liability where there is harm instead of looking for "gotcha" fines on technical violations.

CONCLUSION

The classification of broadband Internet access providers as a Title II telecommunication service requires careful and methodical evaluation of numerous rules, including those around CPNI. The commission should err on the side of restrained rules and limited and clear liability. When it comes to sharing CPNI, carriers should be free to share properly de-identified or aggregated data without restrictions, while personally identifiable data that is appropriate to share should be subject to a basic "opt-out" framework.

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* Federal Communications Commission, *Protecting and Promoting the Open Internet,* GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order (Rel. March 12, 2015) ("*Open Internet Order*") paras. 462-467.
3. 47 U.S.C. § 222.
4. The FCC's initial implementation focused less on consumer privacy and more on the use of local exchange customer data by regional Bell operating companies to market interLATA toll services, which is understandable considering the context of the 1996 Act. The plain text of the statute also makes clear that an animating concern of Congress was interconnecting carriers leveraging other carrier's CPNI for marketing. *For discussion, see* Gerard J. Duffy, "The New CPNI Rules," *Rural Telecommunications* (March-April 2008), 47.
5. *Id.*
6. This shift was largely designed to combat the growth of "pretexting" –the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records. Federal Communications Commission, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking (rel. April 2, 2007) ("*2007 CPNI Order*").
7. *Open Internet Order* para 462. Note that in the Open Internet Order, the commission forborne its own implementing regulations, but decided to apply the section 222 statute itself. When the Open Internet Order becomes effective, broadband Internet access providers will potentially be subject to enforcement action based solely on the statute itself. This report aims to help start the process to bring greater clarity to a new, vague area of liability.
8. 47 U.S.C. § 222(h)(1).
9. *See 2007 CPNI Order, supra* note 6 at para 4.
10. *Open Internet Order* para 462.
11. *See Open Internet Order* fn.1379, *citing* Public Knowledge Dec. 19, 2014 *Ex Parte* Letter at 19.
12. Laura Moy, "What to Take Away from the FCC Settlement with Verizon over CPNI," *Public Knowledge,* September 5, 2014, https://www.publicknowledge.org/news-blog/blogs/what-to-take-away-from-the-fcc-settlement-with-verizon-over-cpni.
13. *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; Daniel Castro, "Data Privacy Principles for Spurring Innovation" (Information Technology and Innovation Foundation, June 2010), http://www.itif.org/publications/data-privacy-principles-spurring-innovation.
14. The 2013 CarrierIQ Declaratory Ruling helped shed some light on the scope of liability, but difficult questions remain to be addressed given the different context and rapidly changing technology. *See* Federal Communications Commission *Implementation of the Telecommunications Act of1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling (rel. June 27, 2013).
15. For discussion of self-regulation in the context of online behavioral advertising generally, *see* Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising" (Information Technology and Innovation Foundation, December 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.
16. 47 U.S.C. § 222(c)(2).
17. Generally the commission has interpreted a notice and opt-out procedure as comporting with the statute, and has flexibility in its interpretation. For example, in the 2007 CPNI Order, the commission changed its mind to require opt-in for the sharing of CPNI with joint venture and contractors in attempts to curb pre-texting. *See 2007 CPNI Order supra* note 6.

18. *See 2007 CPNI Order, supra* note 6 for discussion of the limited scenarios under which the general implied consent rule had been elevated to a requirement of express consent.
19. *See* Ann Cavoukian & Daniel Castro, "Setting the Record Straight: De-Identification Does Work" (Information Technology and Innovation Foundation, June 2014), http://www.itif.org/publications/setting-record-straight-de-identification-does-work.
20. *See* Daniel Castro & Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-how-when-regulators-intervene.pdf.
21. Again, these issues of appropriate CPNI scope featured prominently in the Carrier IQ Declaratory Ruling, but the complexity and continued evolution of broadband networks warrant a re-evaluation of those decisions. *See 2013 CPNI Order supra* note 14.
22. *See* Castro & McQuinn, "How and When Regulators Should Intervene" *supra* note 19.

ABOUT THE AUTHORS

Doug Brake is a Telecommunications Policy Analyst with the Information Technology and Innovation Foundation. He specializes in broadband and wireless policy, with interests in net neutrality and spectrum rights definitions. 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 and Director of the Center for Data Innovation. Mr. Castro writes and speaks on a variety of issues related to information technology and internet policy, including privacy, security, intellectual property, internet governance, e-government, and accessibility for people with disabilities. 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.

Dr. Robert Atkinson is the President of the Information Technology and Innovation Foundation. He is also the author of the book, *The Past and Future of America's Economy: Long Waves of Innovation that Power Cycles of Growth* (Edward Elgar, 2005). Dr. Atkinson received his Ph.D. in City and Regional Planning from the University of North Carolina at Chapel Hill in 1989.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

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