OPEN TECHNOLOGY INSTITUTE

THE FCC'S ROLE IN PROTECTING ONLINE PRIVACY

AN EXPLAINER

JANUARY 2016

Acknowledgments

This report was prepared in collaboration with Upturn. We thank Harlan Yu, Linda Zang and David Robinson for their contributions to this report.

About New America

New America is dedicated to the renewal of American politics, prosperity, and purpose in the Digital Age. We carry out our mission as a nonprofit civic enterprise: an intellectual venture capital fund, think tank, technology laboratory, public forum, and media platform. Our hallmarks are big ideas, impartial analysis, pragmatic policy solutions, technological innovation, next generation politics, and creative engagement with broad audiences.

Find out more at **newamerica.org/our-story**.

About the Open Technology Institute

The Open Technology Institute at New America is committed to freedom and social justice in the digital age. To achieve these goals, it intervenes in traditional policy debates, builds technology, and deploys tools with communities. OTI brings together a unique mix of technologists, policy experts, lawyers, community organizers, and urban planners to examine the impacts of technology and policy on people, commerce, and communities. Our current focus areas include surveillance, privacy and security, network neutrality, broadband access, and Internet governance.

Find out more at **newamerica.org/oti.**

Contents

THE ISSUE: FORCING CONSUMERS TO CHOOSE BETWEEN PRIVACY AND INTERNET ACCESS

Share intimate details of your life with strangers, or be shut out of the Internet.

ISPs today are fast gaining the technical capacity to force consumers into this dilemma. That situation is bad for consumers, bad for the public interest, and getting worse as the technologies of tracking continue to improve.

Fortunately, the FCC's decision to reclassify Internet access as a common carriage service under Title II of the Communications Act gives the Commission powerful new tools to protect the privacy of online life.[1] Specifically, the FCC has a statutory mandate[2] to shield the sensitive information that a common carrier learns about customers in the course of providing a telecommunications service.[3] This information includes both personal information about customers, termed "proprietary information" under the law, and information about a customer's use of the service that she has no choice but to provide in the course of receiving service, known as "Customer Proprietary Network Information" (CPNI).[4] Providers covered by the statute have a general duty to protect all proprietary information, including CPNI. Additionally, before a covered provider can use CPNI for any purpose other than providing the service, it must obtain the customer's consent.[5]

Authorized by Section 222 of the Communications Act and first applied to telephone service, the FCC's existing CPNI rules protect information including the numbers a customer texts or calls, for how long, and when.[6] Phone companies can use that information to connect calls and calculate billing, but cannot share or use it for other purposes unless they get the customer's permission. The FCC has also interpreted the provisions of Section 222 that require carriers to protect "proprietary information" to extend more broadly to "private information that customers have an interest in protecting from public exposure."[7] Although Section 222 has traditionally been applied to telephony, Congress designed the provision to be flexible.[8]

With reclassification of broadband as a Title II service, Section 222 now applies to broadband Internet access service providers—a category that includes both wireline providers such as cable companies, and wireless service providers that offer mobile Internet services. As the Commission has long recognized, "[c]onsumers' privacy needs are no less important when consumers communicate over and use broadband Internet access than when they rely on [telephone] services."[9]

The application of Section 222 privacy protections to ISPs is important and timely. Already, ISPs are developing and expanding ways to monetize their subscribers' personal lives and daily habits by using subscriber information for lucrative non-service-related purposes.[10] On the wireless side, at least one mobile broadband provider has used its unique control over Internet access to proactively inject persistent individual identifiers into outgoing mobile web traffic, which enables third-party firms to silently track subscribers' patterns and habits.[11]

From their position as gatekeepers to the Internet, ISPs have a uniquely detailed and comprehensive view of all of subscribers' unencrypted online communications, personal habits, and daily lives. Subscribers have no choice but to share this information; to gain access to the Internet, they must connect through an ISP. By the nature of their role, ISPs can therefore build a comprehensive picture of users' online activities, ranging across time, across different sites, services, and devices—from their streaming video habits on Netflix, to the frequency with which they request online banking services, to the times of day they are most active on Facebook and other websites.

In addition to the unique scope and insight they have into subscribers' activities, ISPs also face little competition in the market for last mile consumer-facing broadband services.[12] On the wireline side, more than 55 percent of Americans have just one option for service at speeds above 25 Mbps, the minimum necessary for today's video-intensive applications.[13]

Subscribers have slightly more carrier options on the wireless ISP side, with four major national wireless carriers and a small number of mobile network resellers (MVNOs) that lease capacity from existing wireless carrier infrastructure. However, even the MVNOs may be subject to the tracking systems now being rolled out by those four major wireless ISPs.[14] Moreover, wireless service has inherent bandwidth constraints that make it a far from ideal substitute for wireline service.

Technological trends that point toward ever more data-intensive services will only widen the opportunity and productivity gaps between those consumers who enjoy truly broadband wireline service and those who must make do exclusively with the more limited speeds and data caps imposed by wireless ISPs. One consequence of this lack of consumer choice is that subscribers who object to their ISP's data privacy policy have few alternatives for connecting to the Internet. In order to participate in the free exchange of information, ideas, and services, consumers have no choice but to entrust every aspect of their online interactions to their Internet service providers.

Section 222 recognizes the special nature of the relationship a subscriber has with a common carriage telecommunications service. Subscribers have no choice but to share the minute details of their daily communications to a carrier because doing so is necessary in order to communicate.[15] Carriers must protect that information.[16] And if a carrier wants to use CPNI for a different purpose,[17] or wants to share it with a third party,[18] the carrier must obtain the customer's affirmative consent.[19] These obligations ensure that subscribers can rely on confidentiality for their personal information, and do not have to sacrifice privacy in order to use the service.

By creating strong privacy rules for broadband Internet service, the FCC can protect the public interest and ensure baseline privacy protections for every Internet user. Such rules can ensure that users, and not service providers, will decide what happens to their personal information online.

WHAT CAN INTERNET PROVIDERS AND THEIR PARTNERS LEARN ABOUT SUBSCRIBERS?

Because of their special role handling all of a user's Internet traffic, ISPs have a uniquely detailed and comprehensive perspective on the activities of their subscribers. Unlike individual IP-based services and applications, ISPs are able to collect a constant stream of information across multiple devices and multiple platforms. Even when subscribers shut off a device or program, ISPs can place that silence in the context of the subscriber's historical daily usage patterns. At a technical level, ISPs have a wide range of ways to gather and compile an extremely detailed profile about each subscriber.

Content of All Unencrypted Internet Traffic

Each time a user accesses a website or uses an Internet application (such as sending email using Outlook), the user's computer makes one or more connections to servers across the Internet. Because each connection must travel through the user's ISP, the ISP has the opportunity to monitor all the information that travels across that connection.

Some of these connections are encrypted, and some are not. When a connection is encrypted, the information being sent is scrambled just before leaving the user's computer, and unscrambled as soon as it reaches the server. (Similarly, on the return path, the server scrambles information before sending, and the user's computer unscrambles upon receipt.) In between, the ISP can only see the scrambled information.

Whether a particular connection is encrypted depends largely on how individual servers are configured. Some servers require the use of encryption. In other cases, encryption may be an option, or may be completely unavailable, forcing users to either connect insecurely or not at all. Rarely do users actively decide whether a connection is encrypted or not; that decision is usually made by the user's computer and the server, automatically, whenever a connection is initiated.

Most of today's Internet traffic travels through ISPs unencrypted. Whenever a connection is unencrypted, the information that travels across that connection is exposed to the ISP. This means that ISPs have the technical capacity to learn about the articles that users read online, the videos that they watch, and the products they shop for. As of April 2015, an estimated 65 percent of all downstream Internet traffic in North America remained unencrypted.[20]

In some circumstances, even the content of the private chats and e-mails that users send to their family and friends are exposed to their ISP. Many e-mail applications make unencrypted connections to mail servers, allowing every piece of mail that is sent or received by the user to be intercepted and read by the ISP.[21] This empowers the ISP to observe sensitive personal and business information about their subscribers and their subscribers' contacts.

An ISP could even gain a subscriber's login credentials to a website or service. On some websites, the login process sends a username and password to the server without using encryption. If an ISP is routinely storing or analyzing subscribers' traffic, the subscriber's login credentials could be swept up during those activities. Even if the subscriber logs in using an encrypted connection, some websites do not encrypt subsequent connections, which means that the cookies that allow the user to remain logged in would be exposed to the user's ISP. If those cookies are swept up, they could be used to log in and impersonate the user.

It is often difficult or impossible for users to tell whether a particular connection is encrypted or not. The most familiar indication to most users is the lock icon in their web browser's URL bar. But for many other applications—including mobile applications and Internet-enabled appliances—no similar signal may be available for the user.

Destination Information for All Internet Traffic

Driven in part by the Snowden disclosures, Internet websites and services are increasingly implementing and requiring the use of encrypted connections. But even as more connections are encrypted in the future, ISPs will still be able to track in detail the websites and services their subscribers access.

The domain name system (DNS) is an integral part of today's Internet. The purpose of DNS is to translate human-readable domain names (such as plannedparenthood.org) into an IP address (such as 66.151.111.232 — the destination address for Planned Parenthood's web server). In order to visit plannedparenthood.org, the user's computer must first connect to a DNS server and ask for the destination site's current IP address.

> ***Driven in part by the Snowden disclosures, Internet websites and services are increasingly implementing and requiring the use of encrypted connections. But even if more connections are encrypted in the future, ISPs will still be able to track in detail the websites and services their subscribers access.***

ISPs frequently own and operate the DNS servers that their subscribers use.[22] By default, when a user's computer connects to an ISP's network, the network automatically configures the computer to use the ISP-owned DNS server. 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.

Domain names, of course, can expose intimate details about the subscriber's health (plannedparenthood.org), finances (acecashexpress.com, particularly if accessed before each payday), political views (joinnra.nra.org), and many other sensitive attributes. A subscriber's history of domain name lookups could also be used to more accurately predict certain attributes about a subscriber like gender, age, race, income range, and employment status. Without appropriate regulatory safeguards for broadband traffic data such as DNS queries, these inferences could be made available on the open market, without specific notice or affirmative consent from the subscribers whose lives are being examined.

User Connection Patterns: Frequency, Timing, and Location of Connections

Under typical circumstances, an ISP will see each site a user visits, and when and for how long. This information can reveal the times of day when a subscriber habitually goes online, and can be used to detect whether there has been a sudden shift in a subscriber's behavior. Such a shift could indicate that a major life event has occurred, e.g., that the subscriber likely just had a child, or likely lost her job. Such major events could be inferred from the frequency and timing of a subscriber's Internet use, particularly when combined with other information available to ISPs.

For a wireless subscriber, the ISP could also continuously track her location information. Cell phones repeatedly send signals to nearby cell towers, allowing service providers to approximate location. By combining information from multiple towers, a wireless ISP can track a subscriber's movements throughout each day, often to within a city block in many urban environments.

Because of the revealing nature of location information, a wireless ISP subscriber can typically control when, and with which apps, to share her location. It is also possible to turn off all location services using the location settings on the phone. But such settings do not impact an ISP's access to location information: phones will continuously send signals to cell towers in order to receive mobile service, regardless of the user's location preferences. Without clear privacy rules, an ISP might elect to sell subscribers' location histories without appropriate notice or consent. If wireless ISPs were to gather and sell location histories absent meaningful notice and consent, then the feeling of control created by a phone's location privacy settings could be reduced to a comforting illusion.

HOW CAN THIS INFORMATION BE ABUSED?

On its own or in combination with other consumer data, the information that Internet subscribers have no choice but to share with their ISPs could be abused. Some ISPs could elect to funnel subscriber data into a data brokerage marketplace, where the data would find its way to the firms most able to combine, analyze, and extract value from it. Some ISPs will use customers' information to inform their own behavioral advertising efforts.[23] ISPs that wish to extract more value from user data could partner with analysis firms to gain greater insight into subscribers' lives. Without clear and comprehensive privacy rules governing appropriate uses of the detailed data subscribers share with their ISPs, ISPs, their partners, or downstream data purchasers could use subscriber information for a number of troubling non-service-related purposes.

Targeting the Newly Unemployed

Wireline ISPs know when the subscriber uses the web from a particular physical location, and where the subscriber goes online. If a home connection, normally dormant during business hours, suddenly starts seeing significant mid-day use during the week, and some of those requests are going to job search sites, the information could allow the ISP (or a third party analytics partner) to infer that the subscriber has lost a job. That information could be sold to predatory financial vendors or other troubling actors—a chain of events whose root cause would never be visible to the subscriber herself. Thanks to their unique position as access providers, ISPs can detect even subtle changes to a subscriber's daily use habits.[24]

Sharing Information About Personal Health Conditions

A cluster of subscriber visits to a doctor's website or to a prescription refill page could allow the ISP or a data broker partner to infer that the subscriber or someone close to the subscriber has been diagnosed with a new medical condition, such as a heart condition, depression, or another personal health condition. In a worst case scenario, ISPs could sell this package of information and inferences to healthcare companies or to potential employers, all without authorization from the subscriber herself.

Gathering Information from the Internet of Things

With the rise of the Internet of Things, the information about everyday habits that subscribers share with ISPs will continue to grow. Traditional home appliances and parts—from thermostats to televisions to door locks—are already "smart." Cars are now commonly Internet-equipped. New personal health devices like step and sleep trackers, and newly improved devices like pacemakers, now send and receive health data over the Internet.

In the same way that ISPs could monitor a subscriber's unencrypted web browsing behavior, or make inferences based on specific Internet usage patterns, ISPs that elect to monitor their subscribers' traffic will gain profound new abilities to monitor subscribers even when they are not actively using their desktops or mobile phones. Unlike any other actor in the Internet landscape, ISPs are positioned to see the Internet traffic generated by all of these devices—a stream of data that offers detailed insight into users' daily lives.

Increasing the Cost of Doing Business on the Internet

ISPs' role as Internet gatekeepers also enables them to obtain intimate insight into the otherwise confidential details of other companies' dealings with their customers, including companies that compete directly with the ISP and its affiliates in other markets. For example, AT&T, which markets its own version of a home security system, could use its position as an ISP to surveil private business communications that pass between its subscribers and a home security company that competes with AT&T in that market.[25] It might elect, for example, to track which users seek technical support on the competitor's site, and extend special offers to those users. Such behavior—which is technically feasible—could gravely undermine the Internet's effectiveness as an open engine of commerce. It also runs counter to the basic expectations that Congress, businesses, and consumers have of common carriers entrusted with maintaining the key communications infrastructure of the 21st century.

WHAT WOULD CONSUMER-FRIENDLY PRIVACY RULES FOR BROADBAND SAY?

Strong privacy rules will help to maximize consumers' trust in ISPs—trust that is crucial for free and open speech to flourish on the Internet. There are already rules implementing Section 222 on the books for phone carriers, and the FCC has committed to promulgating new rules for ISPs. Done right, new privacy rules will provide the baseline privacy protections subscribers need to retain meaningful control over intimate details about their personal lives and individual habits. ISPs are free to offer even more privacy protections. In the meantime, certain baseline protections should be provided to all subscribers, ensuring that subscribers are not routinely required to give up control over their personal information as a condition of going online.

Start with an Inclusive Definition of CPNI

A clear and inclusive definition of CPNI is the starting point for a robust modern regime of consumer privacy protections.[26] At a minimum, the FCC's new privacy rules for broadband should be at least as protective of consumer information as the FCC's CPNI rules for traditional telephone services. This means that the FCC should include within the definition of broadband CPNI those categories of Internet subscriber information that fit squarely within the statutory definition of CPNI,[27] including, for example, subscriber location information, sites visited, specification of connected devices, and time, amount, and type of Internet traffic.[28] Moreover, the FCC should also take into account the significant new risks to consumers in the broadband context, and expand the definition of CPNI where appropriate. In addition, the FCC should adopt rules formalizing the definition of "proprietary information" as interpreted in the recent enforcement action against TerraCom and YourTel.[29]

Require "Opt-In" Subscriber Consent for Non-Service-Related Uses of CPNI

The FCC should preserve subscribers' control over their own information. An "opt-in" consent disclosure regime allows subscribers to decide who should get access to the uniquely intimate and comprehensive constellation of personal information visible to their ISP, and what that information can be used for. In order for subscriber control to be meaningful, ISPs must provide their subscribers with accurate and reasonably specific descriptions of the nature of the information to be disclosed, the purpose for which their information will be used, and the identity of the third party to whom the disclosures will be made. An opt-in disclosure regime will enable subscribers to have a say in third-party access to their personal information, while providing a mechanism for ISPs to market some of their collected data.

Require ISPs to Disclose CPNI to Subscribers

In order for subscribers to make informed opt-in decisions, they need to have the ability to access all of the proprietary information and CPNI that their ISP collects about them. As explained above, ISPs can collect and extract extremely detailed and sensitive information about a subscriber's private life, and it may come as a surprise to many subscribers that their ISP is in possession of such information. Subscribers cannot make well-informed decisions about their personal information unless they are fully aware of exactly what that information contains. In order for an opt-in regime to protect subscribers, it must be paired with a subscriber's right to access her own CPNI from her ISP. The FCC already has the authority to promulgate such rules under section 222(c)(2), which requires every telecommunications carrier "to disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer."[30]

Include Baseline Requirements for Data Security and Breach Notification

Subscribers have a right to know when their ISP has failed to protect their personal information, and to demand timely remedial action from their carrier. The FCC should implement data security and breach notification requirements for ISPs similar to the FCC's existing procedures for telephone carriers. A data breach notification requirement will protect consumers by letting them know when their personal information has been compromised. These requirements promote transparency and encourage ISPs to proactively secure subscriber information against increasingly sophisticated outside attacks.

Include a Clear Process for Consumer Complaints

Subscribers need access to a formal complaint process for addressing ISP violations of law. The FCC has successfully administered a complaint process for consumers in the context of other telecommunications carrier services, including wireline and wireless telephony.[31] A similar process for wireline and wireless broadband ISP subscribers would aid the Commission in more effectively addressing violations. Without a formal complaint process, individual subscribers would have few means of obtaining proper redress. A formal, well-administered consumer complaint process would also enable the FCC to deploy its enforcement resources more effectively to address the most egregious violations.

Bar ISPs from Charging Subscribers a Premium for Baseline Privacy Protections

These suggested privacy protections define a baseline that should be made available to all Internet subscribers, regardless of their income and socioeconomic status. The threat of ISPs charging a privacy premium is not theoretical—AT&T has already experimented with this model. The FCC should bar ISPs from charging their subscribers a premium for these baseline protections. Without such a prohibition, the basic privacy protections designed to foster the Internet as a forum for free and open speech could become less available to the economically disadvantaged. Wealth-based disparities in communications freedom could in turn reinforce the social and political disadvantages that already challenge the poor.

CONCLUSION

Internet Service Providers are different. They are different from other online players like Apple, Facebook, or Google, both because of their unique role as Internet gatekeepers and because of the nature of the market for consumer-facing last mile Internet service. Their umbrella-like ability to capture individual interactions over the Internet and all aspects of an individual subscriber's daily use patterns is notable. And unlike other actors in the Internet ecosystem, wireline and wireless ISPs are always able to connect individual Internet use patterns to a subscriber's real name, address, phone number, and billing history.[32]

> **With its rulemaking authority, the FCC should set privacy baselines that help to define the minimum standards that Americans can expect from their ISPs.**

With its rulemaking authority, the FCC should set privacy baselines that help to define the minimum standards that Americans can expect from their ISPs. In the long run, the adoption of these basic rules will encourage more Americans to engage in the modern Internet by offering subscribers control over the personal data that they have no choice but to reveal to their common carriers. A clear regulatory framework will ensure that the Internet continues to grow as the essential communications network millions of Americans already recognize it to be—a network where free and open speech flourishes.

NOTES

1. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 47 U.S.C.); Protecting and Promoting the Open Internet, No. 14-28, ___ FCC Rcd. ___, 2015 WL 1120110 (F.C.C. Feb. 26, 2015) (reclassifying broadband Internet service providers as common carriers under Title II of the Communications Act).

2. *See* H.R. Rep. No. 104- 458, at 204 (1996) (Conf. Rep.) [hereinafter Conference Report] (Congress enacted section 222 to "define three fundamental principles to protect all consumers. These principles are: (1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information").

3. *See* H.R. Rep. No. 104-204, at 90 (1995) (stating that the purpose of Section 222 is to balance "the need for customers to be sure that personal information that carriers may collect is not misused" with customers' expectation that "the carrier's employees will have available all relevant information about their services").

4. Section 222 defines "customer proprietary network information" as "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 "information contained in the bills pertaining to telephone exchange service or telephone toll services received by a customer of a carrier." 47 U.S.C. § 222(h)(1)(B)-(A) (2012).

5. However, Congress provided four exceptions where consumer consent is not required. For instance, providers can use CPNI in order "to initiate [and] render . . . telecommunication services," and to provide call location information for emergency 911 services. *See* 47 U.S.C. § 222(d) (2012).

6. *Infra* note 36.

7. *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 at ¶ 14 (2014).

8. 47 U.S.C. § 222(a) (2012) ("[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers. . .").

9. *Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities et al.*, CC Docket Nos. 02- 33, 01-337, 95-20, 98-10, WC Docket Nos. 04-242, 05-271, Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd at 14930, ¶ 148 (2005).

10. *See, e.g.*, Julia Angwin & Jeff Larson, *Verizon's Zombie Cookie Gets New Life*, **ProPublica** (Oct. 6, 2015), https://www.propublica.org/article/verizons-zombie-cookie-gets-new-life (noting that "Verizon said in a little-noticed announcement that it will soon begin sharing the profiles with AOL's ad network, which in turn monitors users across a large swath of the Internet."); Emily Steel & Sidney Ember, *Verizon's Deal for AOL is a Push Into the Technology of Advertising*, **New York Times** (May 13, 2015), https://www.nytimes.com/2015/05/14/business/media/verizons-deal-for-aol-is-a-push-into-the-technology-of-advertising.html ("with Verizon, AOL would gain access to a wealth of data on consumers that it could use to personalize and target marketing messages").

11. *E.g.*, Natasha Singer & Brian Chen, *Verizon's Mobile 'Supercookies' Seen as Threat to Privacy*, **New York Times** (Jan. 25, 2015), https://www.nytimes.com/2015/01/26/technology/verizons-mobile-supercookies-seen-as-threat-to-privacy.html. *See also* Letter from Thomas Wheeler, Chairman, Fed. Commc'n Comm'n, to Senator Edward J. Markey (Mar. 23, 2015) (discussing "the use by Verizon of a mobile tracking technology and its reported exploitation by a third-party advertising company"). At least one other wireless company, AT&T, has experimented with a similar subscriber tracking program. *See* Kashmir Hill, *AT&T Says It's 'Testing' Unique Tracker on Customers' Smartphones*, **Forbes** (Oct. 28, 2014), https://www.forbes.com/sites/kashmirhill/2014/10/28/att-says-its-testing-unkillable-tracker-on-customers-smartphones/.

12. *See* Fed. Commc'n Comm'n, **Broadband Statistics Report: Number of Providers by Speed Tier 5** (2015). *See also* Susan Crawford, *Comcast's Time Warner Deal is Bad for America*, **Bloomberg View** (Feb. 13, 2014), https://www.bloombergview.com/articles/2014-02-13/comcast-s-time-warner-deal-is-bad-for-america ("[F]or the vast majority of businesses in 19 of the 20 largest metropolitan areas in the country, their only choice for a high-capacity wired connection will be Comcast"). The high cost of entering this market means that existing broadband providers are unlikely to face competition from new entrants in the near future, further limiting incentives for existing carriers to be responsive to subscriber privacy concerns. *See, e.g.*, Jonathan E. Neuchterlein & Philip J. Weiser, **Digital Crossroads 8** (2d ed. 2013) (noting that "barriers [to entry] are particularly high--and the rationale for prophylactic regulation therefore strongest--in the case of physical telecommunications networks that provide last-mile transmission to individual homes and businesses").

13. *See* Thomas Wheeler, Chairman, Fed. Commc'n Comm'n, The Facts and Future of Broadband Competition (Sep. 4, 2014). ("At 25 Mbps, there is simply no competitive choice for most Americans. Stop and let that sink in . . . three-quarters of American homes have no competitive choice for the essential infrastructure for 21st century economics and democracy. Included in that is almost 20 percent who have no service at all!")

14. *See* Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customer*, **Electronic Frontier Foundation** (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh (noting that "Verizon appears to inject the X-UIDH header even for customers of Straight Talk, a mobile network reseller (known as a MVNO) that uses Verizon's network. Customers of Straight Talk don't necessarily have a relationship with Verizon").

15. 47 U.S.C. § 222(b), (c)(1) (2012) (permitting carriers to use CPNI for the purpose of providing the telecommunications service).

16. 47 U.S.C. § 222(a); *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014).

17. *Id.* (general prohibition against the use of CPNI for carrier's own marketing efforts and against disclosure of CPNI for purposes other than the provision of telecommunications services).

18. 47 U.S.C. § 222(c)(2) (2012) (requiring "affirmative written request" by the customer for carrier disclosure of CPNI to a third party).

19. *Id.*

20. *See* Sandvine, Global Internet Phenomena Spotlight: Encrypted Internet Traffic 3 (May 8, 2015). https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.

21. Nearly half (42 percent) of the incoming emails to Gmail servers were unencrypted during transit. Email Encryption in Transit, **Google Privacy Rep.** (Dec. 29, 2015), https://www.google.com/transparencyreport/saferemail/.

22. Even where a subscriber uses a third-party DNS server (rather than the one operated by the ISP) the ISP could still learn the same information by monitoring every DNS request that the subscriber sends over the network. With few exceptions, DNS queries are sent unencrypted and are visible to ISPs. There is no widely used standard to encrypt DNS traffic.

23. *See, e.g.*, Emily Steel & Sidney Ember, *Verizon's Deal for AOL is a Push Into the Technology of Advertising*, **New York Times** (May 13, 2015), https://www.nytimes.com/2015/05/14/business/media/verizons-deal-for-aol-is-a-push-into-the-technology-of-advertising.html ("with Verizon, AOL would gain access to a wealth of data on consumers that it could use to personalize and target marketing messages").

24. *See, e.g.*, Steffen Gebert et al., *Internet Access Traffic Measurement and Analysis 3* (Inst. of Computer Sci., Univ. of Wuerzburg, Conference Paper, 2012) (explaining methodology for collecting and analyzing daytime household Internet usage patterns of 600 individual households using data made available by a German broadband ISP).

25. *See* Declaration of Brian Collins, Thomas F. Hughes and Matthew T. Haymons in Support of Motion for a Stay at ¶ 8, U.S. Telecom Ass'n v. Fed. Commc'n Comm'n, No. 15-1063 (D.D.C. filed May 13, 2015), *available at* https://www.publicknowledge.org/assets/uploads/blog/15.05.13_Motion_for_Stay_Exhibits.pdf ("AT&T also uses the fact that a customer is an AT&T broadband customer to assist its marketing of other AT&T services, such as security services and technical support packages.").

26. Including, for example, the history of sites visited, packet data and communications contents, device specifications, and the timing, frequency, and intensity of broadband use.

27. 47 U.S.C. § 222(h)(1) (2012) (defining "customer proprietary network information" to include "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").

28. This is analogous to the definition of CPNI in the traditional wireline and wireless telephony context, where CPNI includes, among other things, the phone numbers dialed by a customer, the frequency, duration, and timing of phone calls, any services purchased by the customer, location data on where a phone experiences a network event (such as a dialed or received phone call, or a dropped call). *See* Implement. of the Telecomm. Act of 1996, 28 FCC Rcd. 9609, 9617 (2013) (2013 CPNI Order) ("[t]he examples CTIA cites, such as 'data on when and where calls fail' and the 'location, date, and time a handset experiences a network event, such as a dialed or received telephone call' do reveal call details which we conclude do fall within the statutory definition of CPNI"); Implement. of the Telecomm. Act of 1996, 22 FCC Rcd. 6927, 6931 (2007) (2007 CPNI Order) ("CPNI includes information such as the phone numbers called by a consumer [and] the frequency, duration, and timing of such calls"); Implement. of the Telecomm. Act of 1996, 17 FCC Rcd. 14860, 14864 (2002) (2002 CPNI Order) ("[p]ractically speaking, CPNI includes personal information such as the phone numbers called by a consumer, the length of phone calls, and services purchased by the consumer, such as call waiting").

29. *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 at ¶ 14 (2014) (interpreting the provisions of Section 222 that require carriers to protect "proprietary information" to extend to "private information that customers have an interest in protecting from public exposure").

30. 47 U.S.C. § 222(c)(2) (2012).

31. *See* Complaints, **FCC Encyclopedia** (Nov. 4, 2014), https://www.fcc.gov/encyclopedia/complaints (explaining the methods by which consumers can file a complaint and discussing the subjects covered by the complaints process).

32. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010) (explaining why data anonymization techniques fail to protect the identity of individual customers).