Net Neutrality and Privacy: Don't Fear the Reclassification
2015 TPRC – 43rd Research Conference on
Communications, Information, and Internet Policy
Commissioner Julie Brill
September 26, 2015

Good evening. Thank you, Madura, for your very kind introduction. It's an honor to have the opportunity to address all of you at this year's TPRC. Now in its forty-third iteration, this conference has been the locus of a tremendous amount of innovative thinking and spirited debate about all issues connected with the movement of information. The broad range of subject matter in this year's program is truly impressive, and I thank Scott Wallsten and the TPRC Board for inviting me to speak with you this evening.

Since it's Saturday night, and you have had two days of speeches and panels – not to mention the dinner and glass or two of wine that you've had this evening – I know I need to find a compelling topic to keep you all awake. Given the expertise that is present in this room, I think I found the right one: the shape of consumer privacy protections under the FCC's Open Internet Order.

First, let me be clear about where I stand on the basic issues surrounding net neutrality. I support the FCC's goal of preventing the blocking or degradation of sites and services that consumers want to reach. I believe that the Open Internet Order[1] will help to achieve these goals. And I also believe that strong consumer privacy and data security protections are key ingredients of our data-intensive economy, including the practices of broadband providers.

I'm here to deliver two messages. The first is that I welcome the FCC as another cop on the privacy beat. My agency, the Federal Trade Commission (FTC) has been an effective enforcer of these protections ever since the commercial Internet developed in the late 1990s. While one consequence of the FCC's Open Internet Order is that it could become more difficult for the FTC to bring enforcement actions against ISPs based on their data practices, consumer privacy enforcement continues to present a target-rich environment. The Order moves the FTC out of enforcement in a narrow but significant band of commercial activity on the Internet. But even with the Open Internet Order, the FTC keeps its place as the nation's leading consumer protection and privacy agency. Our consumer protection authority extends to the apps, edge services, ad networks, advertisers, publishers, data brokers, analytics firms, and the many other actors whose data practices are part of the delivery of valuable services to consumers but also, in some instances, raise privacy and data security concerns. And, of course, the FTC's jurisdiction extends far beyond that – we have authority over any unfair or deceptive acts affecting commerce, unless specifically carved out from the FTC's jurisdiction.[2]

[1] FCC, In the Matter of Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order (Mar. 12, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf ["Open Internet Order"].

[2] *See* 15 U.S.C. § 45(a).

One thing we have learned through our extensive efforts to enforce laws governing the data collection and use practices in the digital age is that it requires enforcement agencies to have an ever-increasing level of technical sophistication. That is why we created a chief technologist position at the FTC, and brought in Ed Felten, Steve Bellovin, Latanya Sweeney and Ashkan Soltani to serve in this role. And it is why we have created an Office of Technology Research and Investigation.[3] The FCC also has the capability – technological expertise and understanding of the industry players – to bring a level of sophistication to the analysis of ISPs' data collection and use practices.

Where the FTC and FCC overlap in other enforcement areas, we have a successful working relationship, and I have every reason to believe that our good working relationship will continue as the FCC's privacy-related enforcement and policy efforts take shape under the Open Internet Order.

My second message is that the reclassification of broadband Internet access service presents a rare opportunity to discuss consumer privacy in a specific context: the relationship between consumers and their broadband providers. The FCC, other policy makers, companies and advocates should use this opportunity to focus the discussion of privacy under the Open Internet Order on the important consumer privacy issues that are at stake. So, I don't fear reclassification. Indeed, I stand ready to join the discussion that will unfold in the coming months, and help keep it focused on the critical substance of consumer privacy.

Consumer Privacy as an Element of Digital-Age Consumer Protections

But because many of you may be more familiar with the FCC than the FTC, let me say a few words about my agency before I get to this more substantive discussion. The FTC is first and foremost a civil law enforcement agency. We are the nation's leading consumer protection agency, and we share competition enforcement authority with the Department of Justice. Under authority given to us in 1938, the FTC is responsible for protecting consumers from a broad range of "unfair or deceptive acts or practices."[4] Under this authority, which is in Section 5 of the FTC Act,[5] we have brought hundreds of cases against companies for making deceptive claims in advertising. We have shut down scams that falsely promise to deliver credit repair, mortgage relief, business opportunities, and other services that predominantly target vulnerable consumers. And we have been a leader in stopping robocalls and abusive telemarketing practices. Congress has passed laws that ban specific kinds of harmful practices, as is the case with telemarketing.[6] But Section 5 itself is broad and applies even when more specific statutes are on the books.

---

[3] FTC, Press Release, BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection (Mar. 23, 2015), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next.

[4] 15 U.S.C. § 45(a).

[5] *Id.*

[6] *See* Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. 6101-6108 and Telemarketing Sales Rule, 16 C.F.R. Part 310.

The FTC has been an active consumer protection enforcer in the communications space. We have brought more than 30 cases against landline bill crammers,[7] and more recently, obtained settlements with mobile crammers,[8] as well as wireless carriers for their involvement in billing consumers for crammed charges.[9] We obtained judgments totaling hundreds of millions of dollars in these cramming cases. In our settlements with AT&T and T-Mobile alone, the companies paid a total of $170 million in refunds to their consumers.[10]

The FTC's actions in the communications world go well beyond cramming. In January, we settled an action against TracFone to resolve our concerns that TracFone deceived consumers by offering "unlimited" data plans, but then throttled or even cut off mobile data for consumers who went over certain data use thresholds.[11] We have ongoing litigation in federal court in California against AT&T Mobility based on our concerns about AT&T's similar throttling practices.[12]

In addition, since 2003, the FTC has operated the Do Not Call Registry and has taken aggressive enforcement action under the Do Not Call provisions of the Telemarketing Sales Rule (TSR). The FTC has brought more than 100 actions against companies and telemarketers for Do Not Call, abandoned call, robocall and Registry violations. These unwanted calls not only violate consumers' privacy but also often lead to fraud.[13] Many of these scams target minorities,

---

[7] See FTC, Press Release, FTC Testifies Before Congress on Mobile Cramming Issues (July 30, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/07/ftc-testifies-congress-mobile-cramming-issues.

[8] See FTC, Press Release, Mobile Crammers Settle FTC Charges of Unauthorized Billing (Nov. 21, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/11/mobile-crammers-settle-ftc-charges-unauthorized-billing (describing Wise Media settlement); FTC, Press Release, Jesta Digital Settles FTC Complaint it Crammed Charges on Consumers' Mobile Bills Through 'Scareware' and Misuse of Novel Billing Method (Aug. 21, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/08/jesta-digital-settles-ftc-complaint-it-crammed-charges-consumers (describing settlement with Jesta Digital); and FTC, Press Release, FTC Moves Against Massive Mobile Cramming Operation That Heaped Millions in Unwanted Charges on Consumers' Bills (Dec. 16, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/12/ftc-moves-against-massive-mobile-cramming-operation-heaped (describing action against Tatto, Inc.).

[9] *See* FTC, FTC Alleges T-Mobile Crammed Bogus Charges onto Customers' Phone Bills (July 1, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-t-mobile-crammed-bogus-charges-customers-phone-bills; FTC, Press Release, AT&T to Pay $80 Million to FTC for Consumer Refunds in Mobile Cramming Case (Oct. 8, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/10/att-pay-80-million-ftc-consumer-refunds-mobile-cramming-case.

[10] FTC, Press Release, T-Mobile to Pay At Least $90 Million, Including Full Consumer Refunds To Settle FTC Mobile Cramming Case (Dec. 19, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/12/t-mobile-pay-least-90-million-including-full-consumer-refunds; FTC, Press Release, AT&T to Pay $80 Million to FTC for Consumer Refunds in Mobile Cramming Case (Oct. 8, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/10/att-pay-80-million-ftc-consumer-refunds-mobile-cramming-case.

[11] FTC, Press Release, Prepaid Mobile Provider TracFone to Pay $40 Million to Settle FTC Charges It Deceived Consumers About 'Unlimited' Data Plans (Jan. 28, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/01/prepaid-mobile-provider-tracfone-pay-40-million-settle-ftc.

[12] FTC, Press Release, FTC Says AT&T Has Misled Millions of Consumers with "Unlimited" Data Promises (Oct. 28, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/10/ftc-says-att-has-misled-millions-consumers-unlimited-data.

[13] FTC, The Do Not Call Registry – Enforcement, *available at* https://www.ftc.gov/news-events/media-resources/do-not-call-registry/enforcement (last visited Sept. 25, 2015)

elderly consumers, military personnel, and financially vulnerable consumers.[14] We have obtained more than one billion dollars in judgments for consumer redress or disgorgement and nearly $144 million in civil penalties as part of this Do Not Call enforcement program.[15] In addition, we have run four rounds of challenge to the technical community to develop better ways for consumers to block robocalls. The most recent round of this challenge, which we ran under the banner of "Humanity Strikes Back," led to an app that sends unwanted robocalls to a spam repository, allows call filtering, and provides personalized setting options.

Finally, the FTC has kept a close watch on privacy and security issues surrounding the broadband services that connect most U.S. consumers to the Internet. We have investigated whether security vulnerabilities in one broadband provider's modems might have put consumers at risk.[16] Our 2012 Privacy Report highlighted the privacy risks surrounding ISPs' access to comprehensive data about consumers' online activities[17], and we raised concerns about deep packet inspection[18] and uses of geolocation information.

Reclassifying Privacy Protections Under the Open Internet Order

With the reclassification of residential broadband Internet access service as a common carrier service under Title II of the Communications Act, these services are now outside of the FTC's purview. This is because Congress carved out common carriers – along with banks, nonprofits, and a few other entities – from the FTC's jurisdiction.

Although the Open Internet Order puts an important industry sector under Title II and excludes it from the FTC's authority, this is a limited change. It only affects ISPs in their capacity as common carriers. The Order does not affect the FTC's ability to enforce the FTC Act against carriers for activities that are not common carriage services, including some of the most important consumer protection actions we have brought in the past, such as our cramming

[14] FTC, Written Statement for the Senate Committee on Commerce, Science and Transportation Hearing on "Stopping Fraudulent Robocall Scams: Can More Be Done?" (July 10, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-%E2%80%9Cstopping-fraudulent-robocall-scams-can-more-be/130710robocallstatement.pdf.

[15] We have collected $53 million of the more than $1 billion in equitable monetary relief and $49 million of the $144 million in civil penalties obtained in telemarketing-related judgments.

[16] *See* Letter from Maneesha Mithal, Associate Director of the Division for Privacy and Identity Protection, to Dana Rosenfeld, Counsel for Verizon Comms., Inc. (Nov. 12, 2014), *available at* https://www.ftc.gov/system/files/documents/closing_letters/verizon-communications-inc./141112verizonclosingletter.pdf (outlining aspects of Verizon's response and data security program that led FTC staff to close its investigation).

[17] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 56 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (noting that ISPs have "access to vast amounts of unencrypted data that their users send or receive over the ISP's network" and thus are "in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible") [2012 PRIVACY REPORT].

[18] *Id.* at 55-56.

actions against landline and mobile carriers. Moreover, the FTC's authority over consumer protection in wide swaths of the U.S. economy – including "edge" providers – has not changed. Thus, I do not share the concerns of those who believe that the FTC has been dramatically shoved aside.

On the other hand, I think those who are asking the FCC to regulate edge providers as "information services" are asking the FCC to go too far. For example, this past June, several consumer advocacy groups petitioned the FCC to issue rules that require edge providers to honor users' "Do Not Track" requests.[19] Although I have long called on industry to honor Do Not Track requests, I do not believe a rule that the FTC would not be able to enforce is the way to get there. Nor do I accept the premise that ISPs and edge providers need to be under the same – or at least highly similar – privacy regulations in order to avoid giving one an advantage over the other.[20]

A better course to ensuring that broadband providers maintain appropriate privacy protections is to give both the FTC and FCC jurisdiction over common carriage services. This is easy – at least in concept – to do. Congress could simply eliminate the common carrier exemption to Section 5 of the FTC Act.[21] The FTC has called for Congress to take this step for the past decade.[22] The exemption is an artifact. It dates from a time when the horse-and-buggy ruled the streets and the Interstate Commerce Commission was a force to be reckoned with. Today, however, the exemption threatens to leave a gap in the nation's consumer protection laws.

The rationale for creating dual jurisdiction is strong. The FTC and FCC bring different kinds of expertise and have complementary authority that, when brought together, could form a highly effective consumer protection regime. The FTC has the authority to obtain restitution for consumers when they lose money as a result of deceptive or unfair practices. The FCC does not have this authority. We also have vast experience with developing orders that stop bad conduct, and with monitoring those orders to make sure they stick. The FCC, on the other hand, has broad civil penalty authority, which deters companies under its jurisdiction from repeating misbehavior, as well as deterring other players in those sectors that may be considering similar conduct.

---

[19] *See generally* Consumer Watchdog, Petition for Rulemaking to Require Edge Providers to Honor Consumers' "Do Not Track" Requests (June 15, 2015), *available at* http://www.consumerwatchdog.org/resources/fccdntpetiton061515.pdf ["Do Not Track Petition"].

[20] *Contra* Do Not Track Petition, *supra* note 19, at 16 ("If the Commission does not act to regulate the collection of personal information by edge providers, the Commission will in effect be granting a regulatory advantage to the edge providers, implicating concerns of market distortions. In order to maintain regulatory parity, the Commission must impose some rules on edge providers that protect consumers' personal information.").

[21] *See* 15 U.S.C. §§ 45(a)(2), 44.

[22] *See* Prepared Statement of the Federal Trade Commission on FTC Jurisdiction over Broadband Internet Access Services, Presented before the Committee on the Judiciary, United States Senate (June 14, 2006), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-ftc-jurisdiction-over-broadband-internet-access-services/p052103commissiontestimonyrebroadbandinternetaccessservices06142006senate.pdf.

The FTC routinely sorts out areas of overlapping jurisdiction with other agencies. We already share jurisdiction with the FCC on telemarketing and cramming issues. We also have overlapping or adjacent jurisdiction with the Department of Justice, the Consumer Financial Protection Bureau, the FDA, and the Department of Health and Human Services. The FTC has broad and wide experience working things out with other agencies, and I have every reason to believe that the same will hold in our relationship with the FCC under the Open Internet Order.

* * * * * *

A lot more changed than the scope of the FTC's jurisdiction under the Open Internet Order. The reclassification was also an important event for consumer privacy protection. The FCC decided that it would apply section 222 of the Communications Act to ISPs.[23] At the same time, the FCC decided that it would forbear from applying the *rules* that the FCC issued to implement section 222 – the so-called "CPNI rules."[24] As the FCC noted in its Order, the CPNI rules "appear more focused on concerns that have been associated with voice service," as seen, for example, in their definition of "call detail information" that focuses on voice calls.[25] As a result, the FCC decided to forbear from applying the CPNI rules to broadband providers.

Although the FCC has not stated publicly whether it intends to issue a new rule under section 222, it has stated that it is working toward developing "a harmonized privacy framework across various services within the Commission's jurisdiction."[26] I believe that the FTC's privacy policy positions have a lot to offer as the FCC considers what this harmonized framework should look like. First, in our landmark 2012 Privacy Report, we set out a new framework for privacy rights in the digital age.[27] The FTC's framework has three basic elements: privacy by design, effective transparency, and simplified consumer choice. These three elements incorporate many of the individual principles that are part of the Fair Information Practice Principles, including data minimization, data security, access, and accuracy. The report also contains a discussion of deidentification that has become influential in policy discussions around the world.[28] More recently, the FTC also recommended practicing *security* by design, which includes making security part of the design of products and services; testing products for vulnerabilities before shipping or deploying them; training personnel to handle personal information properly; employing a range of security measures to establish defense-in-depth; securing device functionality as well as data; and monitoring for vulnerabilities to devices throughout their

[23] 47 U.S.C. § 222; *see also* Open Internet Order, *supra* note 1, ¶¶ 53-54, 462-467.

[24] *See* 47 C.F.R. part 64.2000; Open Internet Order, *supra* note 1, ¶ 467 (declaring forbearance from applying CPNI rules to broadband Internet access service providers).

[25] *See* Open Internet Order, *supra* note 1, ¶ 467 (discussing the definition of "call detail information," 47 C.F.R. § 64.2003(b)).

[26] FCC, Press Release, Public Workshop on Broadband Consumer Privacy, *available at* https://www.fcc.gov/events/wcb-and-cgb-public-workshop-broadband-consumer-privacy (last visited Sept. 9, 2015).

[27] *See generally* 2012 PRIVACY REPORT, *supra* note 17.

[28] 2012 PRIVACY REPORT, *supra* note 17, at 20-22; Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques (Apr. 10, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

lifecycles.[29] These principles would work equally well for broadband providers. But, because ISPs play a different role and face a much different set of consumer expectations than edge services, I believe we should also consider privacy rules that are tailored for them.

With that basic framework in mind, I would like to draw your attention to some of the specific privacy and data security questions that broadband Internet access raise, irrespective of which agency is responsible for enforcing privacy and data security protections in this sector. I hope that the FCC and all stakeholders will keep these questions – and the general framework that the FTC has developed – in mind as the privacy rules of broadband under the Open Internet Order are developed.

The Case for Strong Privacy Rules for Broadband Providers

So let's look beyond the relationship between the FTC and FCC. Let's even look beyond the context of the Open Internet Order that surrounds the discussion of a privacy rule for broadband providers. Let's focus on the reasons that protecting privacy is critical to consumer trust in the digital age, and the questions that I hope the FCC will consider as it moves forward.

Putting Broadband Providers in Context

The first consideration that should guide debate about privacy rules for ISPs is that ISPs play a central and unique role in most consumers' lives. This recognition is part of the rationale that underlies the Open Internet Order in the first place. It is also a reason to spend a moment putting ISPs in context. Consider what happens when you go through a typical day. You wake up and, before your eyes are really open, start checking your email, the weather, and the news through your smartphone. You can also use your smartphone to adjust the heat and start using appliances, which now communicate with services that monitor your energy use. Meanwhile, your kids use their phones to do last-minute research for school and chat on the latest social networks with their friends. Eventually, you leave the house, and your phone switches from the WiFi connected to your residential fiber connection to your mobile network – provided by the same company as your wireline connection. The mobile network keeps you connected and also keeps track of your location as you drive to the office. And so on throughout the day.

Think of the deeply personal portrait that you could develop from this information. Let's leave aside deep packet inspection for now. Even if an ISP just looks at the IP addresses to which you connect and the time at which connections occur, it can get an intimate portrait of your interests, daily rhythms, habits – as well as those of all members of your household. The ISP can tell whether you're visiting health-related websites, for example, and even whether a health-related question might be keeping you up at night. The ISP can infer the presence of your kids in a household. And as the Internet of Things becomes more deeply embedded in consumers' lives – experts predict that the number of connected devices will double in five years

[29] FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 19-22 (2015) (staff report), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing views of workshop participants) [IOT REPORT].

to 50 billion[30] – data from these connected devices, that reveals your behavior directly or through inference, will become even more detailed and voluminous.

The FTC recognized in its 2012 Privacy Report that broadband providers' status as "a major gateway to the Internet" gives them "access to vast amounts of unencrypted data" that they could use to "develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible" to consumers.[31] Moreover, it may be very difficult for consumers to switch away from their broadband providers if they dislike the provider's data practices, because of the limited choice of high-speed providers that many consumers have. Finally, consumers pay for their broadband service – and pay a lot. The implicit bargain that many view as the basis for "no-cost" consumer services on the Internet – acceptance of targeted advertising in exchange for access to such services – makes much less sense when you are paying 50 dollars or more each month.[32]

All of these considerations lend strong support to the FCC's decision to keep broadband providers under section 222. This law appropriately focuses on the role of carriers, rather than any particular type of activity that might be revealed in CPNI. This is a contrast to many of the other sector-specific privacy laws that we have in the United States. The federal laws governing health, financial, and educational privacy, for example, apply to specific organizations that might handle these kinds of highly sensitive information, such as hospitals, banks, and schools. Although sensitive data now flows freely outside of the protected silos created in HIPAA, GLB, and FERPA,[33] the carrier silo is still meaningful. As a result, the basic structure of section 222 fits the role of ISPs in our data-driven economy.

Addressing Personal Data Use and Disclosure

The second consideration that should guide discussion of privacy principles for ISPs is that personal data *use* deserves attention that is every bit as careful as personal data *disclosure*. To illustrate why both data use and disclosure are integral to privacy protections, let's return to the fictitious ISP I discussed a few moments ago. Suppose our ISP knows that some marketers are very interested in sending health-related ads to consumers, and the ISP wants to capitalize on this business opportunity. Set aside existing laws for just a second. The ISP can choose from two basic approaches.

First, it could determine which of its customers seems to be interested in health-related issues. The ISP could then provide lists of these consumers to edge services, publishers, and

[30] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[31] 2012 PRIVACY REPORT, *supra* note 17, at 56.

[32] *See, e.g.*, Open Technology Institute at New America, The Cost of Connectivity 2014 (Oct. 30, 2014), *available at* https://www.newamerica.org/oti/the-cost-of-connectivity-2014/ (indicating that $50/month is a typical price for residential broadband service in the U.S.).

[33] See Health Insurance Portability and Accountability Act, Pub. L. No.104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.); 15 U.S.C. §§ 6801-6809 and 15 C.F.R. Part 314; Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

marketers. This is a form of disclosure; the ISP informs third parties which of its customers are interested in health issues.

In upholding the CPNI rules in the face of a First Amendment challenge, the DC Circuit gave an eloquent account of how such disclosures threaten individual privacy.[34] The purpose of privacy protections is not simply "preventing embarrassment" by limiting the disclosure of personal information, though the DC Circuit viewed this interest as substantial.[35] The court noted that there is more to privacy, and specifically that "it is widely accepted that privacy deals with determining for oneself when, how and to whom personal information will be disclosed to others."[36]

But limiting disclosure of personal information – whether to prevent embarrassment or to fulfill a broader purpose of maintaining individual self-determination – is not the only aspect of protecting consumers' privacy. The ISP that wants to target certain consumers with health related ads could also *use* personal data about its customers in ways that are privacy-invasive. For example, the ISP itself could occupy the position of a middleman for advertisements by using its knowledge of consumers' health conditions and other interests and behavior to target ads. Such an arrangement may be part of the future that some broadband providers are envisioning for themselves.[37]

Is one approach more privacy-protective than the other? Both of the scenarios that I outlined involve activities that are outside of what many consumers expect of their ISPs. The FTC has long expressed concerns about the ability of services that interact directly with consumers, as well as those that are hidden behind the scenes, such as ad networks and data brokers, to track and profile consumers. Disclosures of a consumer's interest in certain health conditions, her financial status, or her reading and music listening habits for that matter, might be deeply embarrassing. These concerns apply with greater force to broadband providers. The ISP that provides the consumer access to the Internet has all of her web activities at hand. If an ISP were to use this information for the separate purpose of developing marketing profiles or helping marketers to track consumers across different sites and services, I believe that use would be quite out of context of the understood relationship that the consumer has with the ISP, and consequently just as potentially harmful to consumer privacy.

Fortunately, section 222 addresses both disclosure and use.[38] The current CPNI Rule also sets rules for customer approval that are framed explicitly in terms of disclosure and use.[39]

---

[34] Nat'l Cable & Telecom. Ass'n v. FCC, 555 F.3d 996, 1001 (D.C. Cir. 2009) [NCTA v. FCC].

[35] *Id.*

[36] NCTA v. FCC, 555 F.3d at 1001.

[37] *See, e.g.*, Mike Shields and Thoma Gyrta, *Verizon Agrees to Buy AOL for $4.4 Billion*, WALL ST. J. (May 12, 2015), *available at* http://www.wsj.com/articles/verizon-to-buy-aol-for-4-4-billion-1431428458 (discussing relationship of AOL's online advertising technology and Verizon's residential broadband services).

[38] *See, e.g.*, 47 U.S.C. § 222(c)(1) ("Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such

Addressing both disclosure and use in any forthcoming privacy policy under the Open Internet Order will be important for protecting consumer privacy . The critical details – such as whether it makes sense to create heightened protections for the disclosure and use of sensitive consumer data, and the form that consumer consent mechanisms should take – can be developed through discussions in the months to come. For now, I would like to leave you with the thought that the Open Internet Order's animating idea – keeping broadband providers focused on delivering the service that consumers expect – applies to broadband providers' data practices as well.

Security is Paramount.

Data security is the final area that I would like to see front and center in the ongoing discussion of privacy under the Open Internet Order. The security of broadband providers' networks is critical to ensuring that these networks are available for consumers to use at any time of day or night. Broadband providers have strong incentives now to keep their networks up and running. Nothing provokes calls from customers more quickly than a network outage, whether it is the result of a backhoe cutting a fiber optic cable or a denial of service attack on a network gateway slowing traffic to a crawl. In this sense, broadband provider network security is a critical aspect of ensuring that the service delivered to consumers is available and reliable.

The more novel security issues in the broadband context come from the data about consumers that ISPs have. Data security is already a top consumer protection priority for the FTC. Since around 2002, the FTC has brought more than 50 law enforcement actions against companies that, in our view, misrepresented how good their security was or failed to take reasonable measures to secure consumer data.[40] The FTC's initial data security enforcement efforts focused on the financial harms that consumers could suffer when their Social Security numbers or information about their credit cards or bank accounts fell into the wrong hands.[41] But we also focus on security lapses that expose other types of sensitive personal information,[42] including medical information,[43] pharmaceutical records,[44] and our social contacts.[45] More

---

information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.").

[39] *See, e.g.*, 47 C.F.R. § 64.2005.

[40] *See* FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[41] *See, e.g.*, The TJX Cos., Inc., No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter; Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; DSW, Inc., No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; *BJ's Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), *available at* https://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

[42] *See* HTC America, Inc., C-4406 (F.T.C. June 25, 2013) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf.

[43] *See* GMR Transcription Servs., No. C-4482 (F.T.C. Aug.14, 2014) (consent order), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf.

[44] *See* FTC, Press Release, Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (July 27, 2010), *available at* https://www.ftc.gov/news-events/press-

recently, we have drawn attention to the importance of *device* security and have brought one action against a company for allegedly failing to secure the Internet-connected video monitors that it sold to consumers. The FTC will remain vigilant in this area.

ISPs possess data that could expose much of the same information about their customers. Maintaining the privacy of this information is largely hopeless without ensuring that this data is kept appropriately secure. Like other companies that maintain huge amounts of sensitive data about their customers, ISPs could become an attractive target for attackers, and the risk to consumers increases as the amount of data that ISPs store increases. As a result, ISPs should also be held accountable for maintaining appropriate security for consumers' data. I expect that there will be a lot more discussion about whether and to what extent to make data security part of any further policy that flows from the Open Internet Order. At this point, I simply want to make sure that the fundamental connection between privacy and data security is not lost.

* * * * * *

Broadband service is a necessity for many consumers. The FCC is doing the right thing by taking a hard look at the privacy protections that consumers need, as more and more of the details of their online lives flow through their broadband connections. ISPs are not alone in needing to respect their customers' privacy and to keep their data secure, but they play a unique role in the digital ecosystem. The conversation about privacy under the Open Internet Order should proceed from a recognition of this unique role, resulting in strong privacy and security protections. I look forward to more opportunities to discuss the details with all of you, as well as with industry, consumer groups, academics, technologists and, of course, the FCC.

Thank you.

---

releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-and; FTC, Press Release, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), *available at* https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial.

[45] *See* Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), at ¶¶ 34-45 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.