Net Neutrality and Privacy: Challenges and Opportunities
Georgetown Institute for Public Representation and
Center for Privacy and Technology
Symposium on Privacy and Net Neutrality
Commissioner Julie Brill
November 19, 2015

Good morning. Thank you, Angela Campbell, for your very kind introduction. It's an honor to have the opportunity to address all of you at today's Symposium on Privacy and Net Neutrality. Our co-hosts, Georgetown's Institute for Public Representation and Center for Privacy and Technology, have chosen a topic that neatly combines two venerable areas – telecommunications regulations and consumer privacy – into a question of great significance for consumers as well as industry. Given the combined leadership of Alvaro Bedoya, Angela Campbell, Julie Cohen, Laura Donohue, and David Vladeck, such prescience is not surprising.

So, to get things started this morning, let me begin by being 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.

Some of you might want to stop me right now to point out that the Open Internet Order came from the Federal *Communications* Commission (FCC), not from my agency, the Federal Trade Commission (FTC). That is, of course, true. You also may be eager to point out that 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. So, you may ask, why am I embracing the FCC's rule?

There are two reasons. The first is that the Open Internet Order makes the FCC a brawnier cop on the privacy beat, and I welcome its enhanced presence on the scene.

The second reason that I'm eager to focus on privacy under the Open Internet Order is that it presents a rare opportunity to discuss consumer privacy in a specific context: the relationship between consumers and their broadband providers. This is shaping up to be a serious conversation, and I stand ready to help keep it focused on the critical substance of consumer privacy.

Consumer Privacy as an Element of Digital-Age Consumer Protections

Before I get to this substantive discussion, let me say a few words about the FTC and its role in protecting consumers' privacy. The FTC is the nation's leading consumer protection

[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"].

enforcement agency. Under our "unfair or deceptive acts or practices" jurisdiction,[2] 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.

The FTC has also been an active consumer protection enforcer in the communications space. We have been a leader in stopping robocalls and abusive telemarketing practices. The FTC has brought more than 100 actions against companies and telemarketers for Do Not Call, abandoned call, and robocall violations, leading to well over $100 million in penalties. These unwanted calls not only violate consumers' privacy but also often lead to fraud.[3] Many of these scams target minorities, elderly consumers, military personnel, and financially vulnerable consumers.[4]

We have also taken aggressive action against entities that participate in "cramming" — that is, the placement of unauthorized charges on consumers' phone bills. The FTC has brought more than 30 cases against landline bill crammers,[5] and more recently, obtained settlements with mobile bill crammers,[6] as well as wireless carriers for their involvement in billing consumers for crammed charges.[7] 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.[8]

---

[2] 15 U.S.C. § 45(a).

[3] 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)

[4] 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.

[5] *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.

[6] *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.).

[7] *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.

[8] 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.

And the FTC's actions in the communications world extend to the marketing of broadband services. 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.[9] We have ongoing litigation in federal court in California against AT&T Mobility based on our concerns about AT&T's similar throttling practices.[10]

Finally, as you would expect of the nation's leading enforcer of consumer privacy protections, 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.[11] Our 2012 Privacy Report highlighted the privacy risks surrounding ISPs' access to comprehensive data about consumers' online activities[12], and we raised concerns about deep packet inspection[13] and uses of geolocation information.

Reclassifying Privacy Protections Under the Open Internet Order

The FCC's reclassification has placed residential broadband Internet access services 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.

It is important to note how limited the real world impact of this restriction on the FTC's jurisdiction will be. Yes, the Order moves the FTC out of enforcement in a narrow but significant band of commercial activity on the Internet, but it only affects ISPs in their capacity as common carriers. Consumer privacy enforcement, however, continues to present a target-rich environment, and even with the Open Internet Order, the FTC keeps its place as the nation's

[9] 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.

[10] 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.

[11] *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).

[12] *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].

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

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.[14] Thus, I do not share the concerns of those who believe that the FTC has been dramatically shoved aside.

To the contrary, I believe the better argument, one that focuses first on the interests of consumers in 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.[15] The FTC has called for Congress to take this step for the past decade.[16] 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.

And I believe the two agencies would work well to ensure our enforcement efforts are efficient, and that we don't "double team" potential targets. Where the FTC and FCC overlap in other enforcement areas, we have long had a successful working relationship. The FTC and FCC have cooperated since 2003 under a memorandum of understanding (MOU) that applies to telemarketing enforcement issues.[17] And, just this week, the two agencies announced an additional MOU that covers other areas of consumer protection enforcement that we have in common.[18] This new MOU recognizes the agencies' respective areas of expertise, expresses a desire to avoid conflicting or duplicative actions, and outlines specific steps that the agencies will take to remain in sync. An MOU of similar breadth is in place between the FTC and the Consumer Financial Protection Bureau,[19] and it has worked well in terms of formalizing cooperation and providing clarity to stakeholders in the private sector.

---

[14] *See* 15 U.S.C. § 45(a).

[15] *See* 15 U.S.C. §§ 45(a)(2), 44.

[16] *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.

[17] *See* FCC – FTC Memorandum of Understanding on Telemarketing Enforcement, reproduced as an appendix in FTC, Annual Report to Congress for FY 2003 and 2004 Pursuant to the Do Not Call Implementation Act on Implementation of the Do Not Call Registry (Sept. 2005), available at https://www.ftc.gov/sites/default/files/documents/reports/national-do-not-call-registry-annual-report-congress-fy-2003-and-fy-2004-pursuant-do-not-call/051004dncfy0304.pdf.

[18] Memorandum of Understanding on Consumer Protection Between the Federal Trade Commission and the Federal Communications Commission Nov. 2015), *available at* https://www.ftc.gov/policy/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade.

[19] *See* Memorandum of Understanding Between the Consumer Financial Protection Bureau and the Federal Trade Commission (Mar. 2015), *available at* https://www.ftc.gov/policy/cooperation-agreements/ftc-cfpb-interagency-cooperation-agreement.

The rationale for creating dual FTC-FCC jurisdiction over common carriers 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. It also has the authority to issue privacy rules through notice-and-comment rulemaking – something that the FTC cannot do.

The FCC's rulemaking authority – and its source in section 222 of the Communications Act – is a big part of the reason that the reclassification of broadband service was an important event for consumer privacy protection. Section 222 requires telecommunications carriers to provide certain core privacy protections.[20] The Open Internet Order announced that section 222 of the Communications Act applies to ISPs.[21] At the same time, however, the FCC decided that it would forbear from applying the *rules* that the FCC had previously issued to implement section 222 – the so-called "CPNI rules."[22] Instead, as FCC Chairman Wheeler recently stated, the FCC will focus on broadband privacy issues in the "next several months."[23]

* * * * *

I believe that the FTC's privacy policy positions have a lot to offer as the FCC considers what privacy rules for ISPs should look like. First, in our landmark 2012 Privacy Report, the FTC set out a new framework for privacy rights in the digital age.[24] The FTC's framework has three basic elements: privacy by design, effective transparency, and simplified consumer choice. These three elements incorporate many of the Fair Information Practice Principles, including data minimization, data security, access, and accuracy. The report also contains a recommendation about deidentification that has become influential in policy discussions around the world.[25]

---

[20] *See* 47 U.S.C. § 222; Open Internet Order, *supra* note 1, at ¶ 456.

[21] 47 U.S.C. § 222; *see also* Open Internet Order, *supra* note 1, ¶¶ 53-54, 462-467.

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

[23] *See* Mario Trujillo, *FCC to Tackle Broadband Privacy in 'Next Several Months'"*, THE HILL (Nov. 5, 2015), available at http://thehill.com/policy/technology/259232-fcc-to-tackle-broadband-privacy-in-next-several-months (quoting Chairman Wheeler during an interview with Charlie Rose).

[24] *See generally* 2012 PRIVACY REPORT, *supra* note 12.

[25] 2012 PRIVACY REPORT, *supra* note 12, 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.

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 focus on some of the specific privacy and data security questions that broadband Internet access raise, irrespective of which agency is responsible for enforcement. 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.

ISPs Play a Central and Unique Role

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. Throughout the night, a connected onesie has been sending information about your newborn's heart and breathing rate to an app installed on your smartphone. You wake up and, before your eyes are really open, start checking not only stats about your newborn, but also your email, the weather, and the news through your smartphone. You can also use your smartphone to adjust the heat and start your coffee maker, and determine how much energy your household used overnight. Meanwhile, your kids use their phones to do last-minute research for school and chat on the latest social networks with their friends. And in the evening, the streams from your game console and video streaming services dwindle, one by one, as members of your household retire for the night.

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 to 50 billion[26] – data from these connected devices, that reveals your behavior directly or through inference, will become even more detailed and voluminous.

[26] 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.

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.[27] 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.[28]

All of these considerations lend strong support to the FCC's decision to keep broadband providers under section 222which 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.[29] Although sensitive data now flows freely outside of the protected silos created by our education, financial, and health privacy laws, making those silos less and less meaningful,[30] 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

---

[27] 2012 PRIVACY REPORT, *supra* note 12, at 56.

[28] *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.).

[29] *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.

[30] *See, e.g.*, Julie Brill, Commissioner, FTC, Global Regulation of Data Flows in a Post-Snowden World -- Killingstad Global Insights Lecture, Tuck School of Business, Dartmouth College, at 3, 7-8 (Feb. 2015), *available at* https://www.ftc.gov/public-statements/2015/02/global-regulation-data-flows-post-snowden-world-killingstad-global.

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.[31] 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.[32] 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."[33]

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.[34]

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.[35] The current CPNI Rule also sets standards for customer approval that are framed explicitly in terms of disclosure and use.[36]

---

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

[32] *Id.*

[33] *Id.*

[34] *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).

[35] *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 rule 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 already 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.[37] 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.[38] But we also focus on security lapses that expose other types of sensitive personal information,[39] including medical information,[40] pharmaceutical records,[41] and our social contacts.[42]

---

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

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

[37] *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.

[38] *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.

[39] *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.

[40] *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.

[41] *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-

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 stakeholders – industry, consumer groups, academics, and technologists – and, of course, with 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.

[42] *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.