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

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

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

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 so urce in section 222 of the Communications Act is a big part of the reason that the recl assification 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 previous

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 la8irst consit your newborn5.8( )]TJ445 TD 0 Tcn the ev50004isdipacke15 T -.000e rTJ -now -.Ej 12estionsd als

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 comprehe nsive 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

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

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 keep ing 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

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.