FTC-FCC: When is Two a Crowd?

FTC Commissioner Maureen K. Ohlhausen

33rd Annual Institute on Telecommunications Policy & Regulation

December 4, 2015

Thank you, Kathleen, for that generous introduction and thank you to the Federal Communications Bar Association and to the Practicing Law Institute for inviting me to share remarks this morning. I'm sure many of you were here last night for the Chairman's dinner, as was I, so…. Welcome back! Unfortunately, I don't have a funny video to show. But in case I accidentally say anything entertaining, please remember that my remarks are my own and do not necessarily reflect the views of other FTC Commissioners.

D.C. is abuzz with talk about FTC and FCC jurisdiction over privacy and data security. I've been thinking and speaking about that topic for quite a while. Before it was cool. And here before me I have a captive audience of telecommunications lawyers. So it seems appropriate for me to again address that topic and respond to some recent developments.

Background

First, a little background on the FTC and how the FCC/FTC issue arose. The FTC is the leading U.S. enforcer of privacy and data security. We have brought more than 100 privacy and data security cases and more than 150 spam and spyware cases. Our privacy and data security enforcement relies on the FTC's authority to prohibit deceptive or unfair acts and practices in all commerce, with a few key exceptions. Most important here is the FTC's common carrier exemption, which precludes the FTC from bringing actions against common carriers when they are providing common carrier services.

Historically, this exemption didn't include internet service providers, and the FTC has long addressed the practices of ISPs. In the early days of the consumer internet, the FTC brought consumer protection actions against AOL, Compuserve, Prodigy, and other internet access

providers. We've reviewed ISP and cable mergers and transactions with internet components. We've shut down a rogue ISP engaged in illegal activities. And we've investigated a major ISP's data security practices related to potential router vulnerabilities.[1] Most recently, the FTC brought cases alleging that two wireless providers throttled uncongested consumer traffic and thus broke their promises to provide "unlimited data."[2]

As the FTC acted to protect consumers in the ISP space, the net neutrality debate raged. The FTC staff weighed in on this debate, most prominently in 2007. At that time, I was the director of the Office of Policy Planning at the FTC and the head of the Internet Access Task Force. The task force's work culminated in a Commission-approved staff report, "Broadband Connectivity Competition Policy,"[3] which summarized the arguments for and against net neutrality regulation and the technical, economic, and policy issues involved. We also examined the current and future state of broadband competition and analyzed potential broadband provider conduct under various antitrust theories. The report also explored how consumer protection law might address net neutrality concerns. Finally, the report recommended a cautious approach to any new regulation in this area.

Of particular relevance here, the report examined FTC and FCC jurisdiction over internet service providers. In one prescient sentence, the report states, "As the telecommunications and Internet industries continue to converge, the common carrier exemption is likely to frustrate the

---

[1] *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), https://www.ftc.gov/enforcement/cases-proceedings/closing-letters/verizon-communications-inc (summarizing Verizon's response and data security practices, and why FTC staff closed the investigation).

[2] Press Release, Fed. Trade Comm'n, Prepaid Mobile Provider TracFone to Pay $40 Million to Settle FTC Charges It Deceived Consumers About 'Unlimited' Data Plans (Jan. 28, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/prepaid-mobile-provider-tracfone-pay-40-million-settle-ftc; Press Release, Fed. Trade Comm'n, FTC Says AT&T Has Misled Millions of Consumers with 'Unlimited' Data Promises (Oct. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/10/ftc-says-att-has-misled-millions-consumers-unlimited-data.

[3] FED. TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION POLICY (2007) [hereinafter FTC NET NEUTRALITY REPORT], http://www ftc.gov/reports/broadband/v070000report.pdf.

FTC's efforts to combat unfair or deceptive acts and practices and unfair methods of competition in these interconnected markets."[4]

Since that report, the concerns animating net neutrality have not changed much – but the "solutions" certainly have. At our 2007 workshop, a leading advocate for net neutrality regulation stated that she "didn't know anyone who is talking about going back to Title II."[5] Fast forward to late summer, 2014. Although FCC leadership was reportedly not seriously considering Title II reclassification, the idea had gained new prominence. In the fall of 2014, I expressed concern that broadband reclassification would have the unintended consequence of shielding additional activities under the common carrier exemption, and giving some entities a new defense strategy against FTC enforcement actions.[6]

In November 2014, President Obama called on the FCC to reclassify broadband as a Title II common carrier service.[7] The FCC's subsequent 2015 Open Internet Order did so.[8] As a result, the FTC's jurisdiction over ISP practices may now be limited. And ISPs now must comply with many Title II requirements, including privacy and data security requirements. The FCC is currently exploring whether and how to adopt privacy and data security rules for broadband services.

---

[4] FTC NET NEUTRALITY REPORT at 41.
[5] FTC NET NEUTRALITY REPORT at n.683 (quoting Statement of G. Sohn, Tr. I at 125).
[6] *The Communicators* (C-SPAN broadcast Sept. 24, 2014), http://www.c-span.org/video/?321665-1/communicators-maureen-ohlhausen.
[7] *See generally*, White House, Net Neutrality: President Obama's Plan for a Free and Open Internet, https://www.whitehouse.gov/net-neutrality (timeline with Nov. 10, 2014 as the day President Obama called for Title II reclassification).
[8] *See* Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, FCC 15-24 (Mar. 12, 2015).

In the meantime, the FCC has increased privacy and data security enforcement.[9] Indeed, from the outside, it appears that the FCC's enforcement has focused more on privacy and data security issues than on the net neutrality problems the Open Internet Order was intended to address.

When is Two a Crowd? The Two-Rulebook Problem

That brings us to today. How are the new limits on FTC jurisdiction likely to affect consumers? According to some recent observers, this will obviously make consumers better off because we now have two cops on the privacy and data security beat.[10] But having more enforcers isn't always better for consumers. For example, consumers will be worse off if overlapping efforts unnecessarily divert resources from more pressing issues. When two cops are on one beat, another beat may be left vulnerable. Additionally, if enforcers fail to leverage their comparative advantages, consumers will be worse off. For example, one wouldn't expect a homicide detective to do a good job as a tax fraud investigator, and vice versa.

Consumers may also be worse off if the two enforcers have conflicting rulebooks. Economists (and common sense) tell us that if different sets of rules govern competitors, companies subject to the more onerous or unpredictable regime are disadvantaged compared to those outside that regime. This may damage competition or artificially distort the market as companies seek to avoid the more onerous regime.

Although the FCC is still writing its rulebook, there is some evidence that the agencies approach privacy and data security *enforcement* quite differently. For example, the FCC recently

[9] *See, e.g.*, Press Release, Fed. Comm. Comm'n, AT&T to Pay $25 Million to Settle Privacy Investigation (Apr. 8, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf (describing FCC data security and privacy actions in the previous year).

[10] *See, e.g.*, FTC Commissioner Julie Brill, Net Neutrality and Privacy: Challenges and Opportunities (Nov. 19, 2015), https://www ftc.gov/system/files/documents/public_statements/881663/151119netneutrality.pdf.

resolved its first data security case against a cable operator.[11] According to the Order and Consent Decree, the breach at issue involved information about 61 of Cox Communications' more than 6 million subscribers.[12] Amateur hackers social-engineered Cox employees; there was no technical failure involved.[13] Reportedly, no payment information was accessed.[14] The hackers posted some information about *eight* affected consumers on social media.[15] Cox detected and halted the breach within a matter of days and worked with the FBI, who arrested the hacker.[16] The FCC's Order and Consent Decree offers no evidence of any resulting identity theft, or any consumer harm at all. Yet the FCC settlement imposed a $595,000 fine – nearly $10,000 per affected consumer – and extensive compliance measures.[17]

The FCC's approach in the Cox matter differs significantly from the FTC's "reasonable security" approach. I am concerned that what appears to be a "strict liability" data security standard will actually harm consumers. The goal of consumer protection enforcement isn't to make headlines; it is to make harmed consumers whole and incentivize appropriate practices. The costs imposed by a regulator on a legitimate, non-fraudulent company are ultimately born by its consumers. If an enforcement action imposes costs disproportionate to the actual consumer harm, that enforcement action may make consumers worse off if prices rise or innovation slows.

This example suggests that the FTC and FCC rulebooks are different, at least as enforced. Some have argued that it makes sense for the rulebooks to differ, claiming that ISPs are uniquely situated to collect consumer information because all of a consumers' communications travels

---

[11] Fed. Comm. Comm'n, In the Matter of Cox Communications, Order and Consent Decree, DA 15-1241 (Nov. 5, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1241A1.pdf.
[12] Cox Consent Decree at ¶ 9.
[13] Cox Order at ¶ 2.
[14] Thomas M. Lenard, *The FCC flexes its privacy muscles*, THE HILL, Nov. 18, 2015, http://thehill.com/blogs/pundits-blog/technology/260545-the-fcc-flexes-its-privacy-muscles?utm_source=govdelivery.
[15] Cox Consent Decree at ¶ 9.
[16] Cox Consent Decree at ¶ 9.
[17] Cox Consent Decree at ¶¶ 17, 22.

over the ISP's network. If this was ever true, it is not true today. Consumers multi-home and they use multiple ISPs throughout the day. They connect to the internet through their home broadband connection, their mobile device connection, their employer's network, or their local coffee shop's Wi-Fi. Each of these different ISPs has only a fragment of the users' total internet traffic. Thus I question the assumption that an ISP has more comprehensive data than, say, a mobile device that a consumer carries constantly, or a browser that syncs across computers, or a web service that interacts with the same consumer on many different devices. Any data that crosses an ISP's network comes from a piece of hardware or software that has perhaps an equally comprehensive a view of the consumer's activities. Additionally, as internet services increasingly encrypt their traffic, the data ISPs can access diminishes. In short, I am not convinced that ISPs have access to types or volumes of consumer data so unique that it justifies a special set of particularly strict rules.

Others argue that ISPs are unique because consumers pay for their internet service and therefore do not expect ISPs to collect data for other purposes. Even assuming this accurately describes consumer expectations under today's business models, it still isn't a good reason to impose stricter rules that might preclude the development of new business models. Email and search were once primarily paid services. Yet today many consumers choose free, ad-supported versions of these services that collect consumer information. The popularity of such services suggests that many consumers like the option of ad-supported products. As long as ISPs, just like others in the internet ecosystem, tell the truth about how they collect and use consumer data, companies should be free to offer different business models and consumers should be free to choose based on their privacy and other preferences.

In short, I believe there is little evidence that consumers will be better off if one portion of the internet ecosystem operates under a different set of rules from the rest. If there are two cops on the beat, their rulebooks – both as written and as enforced – should be consistent.

Looking Ahead

If we have to choose a rulebook for privacy and data security, it will probably come as no surprise to anyone here that I believe there are significant advantages to the FTC's tried and true approach. We use case-by-case enforcement, applying general legal principles to specific facts, constrained by certain institutional features and a focus on addressing real consumer harm. In dynamic, innovative industries like internet services, an ex post case-by-case enforcement-based approach is far better than ex ante prescriptive regulation. It mitigates the regulator's knowledge problem and allows legal principles to evolve incrementally.[18] A case-by-case approach also focuses on actual, specifically pleaded harms rather than having to predict future hypothetical harms. And a case-by-case approach reduces the incentive for companies to ask regulators to raise rivals' costs.

Of course, case-by-case enforcement without constraining principles and processes is problematic. FTC enforcement seeks to balance flexibility and predictability. Our data security and privacy cases are based on our deception and unfairness authority – two long-standing legal concepts that are themselves hemmed in by precedent, statute, and by our own policy statements. Our complaints and settlements are analyzed not just by lawyers but also by our Bureau of Economics and must be approved by the Commissioners. These institutional features build consensus and limit overreach. And perhaps most importantly, the FTC focuses on consumer harm, both when considering whether to bring a case and in calculating remedies. Focusing on

[18] *See* MAUREEN K. OHLHAUSEN, THE FCC'S KNOWLEDGE PROBLEM: HOW TO PROTECT CONSUMERS ONLINE, 67 Fed. Comm. L.J. 203 (Apr. 2015), https://www.ftc.gov/system/files/documents/public_statements/818521/1509fccohlhausen.pdf.

consumer harm not only ensures that enforcement actually makes consumers better off, it also creates more business certainty.

FCC rules that followed these high-level principles, and in particular an emphasis on limiting action to addressing real consumer harm, would do a lot to align the rulebooks of the cops on the beat.

FCC/FTC MOU

Let me quickly address the recently released Memorandum of Understanding, or MOU, between the FCC and the FTC.[19] As an agency of general jurisdiction, the FTC often needs to coordinate with other agencies, and MOUs facilitate that coordination. The new FTC/FCC MOU largely formalizes already existing processes. There is one piece of interesting substance: I believe this MOU is the first time that FCC staff has acknowledged that the FTC's common carrier exemption is an activity-based (as opposed to status-based) exemption.

While the MOU formalizes coordination, it does not provide any of the principle- or process-based constraints that I have just discussed. In short, it does not solve the two-rulebook problem. This problem may be resolved by the D.C. Circuit, which, in just a few minutes, will hear oral arguments in the challenge to the open internet rules. Or, the FCC's new rules may resolve some of the concerns. In any case, I would welcome Congressional clarification on how to protect consumers' privacy and data security in the ISP context. Whatever the solution, my hope is that the two-rulebook problem is resolved in a manner more thoughtful and transparent than how it was created: as a side-effect of the net neutrality rulemaking.

[19] Press Release, Fed. Trade Comm'n, FTC and FCC Sign Memorandum of Understanding For Continued Cooperation on Consumer Protection Issues (Nov. 16, 2015), https://www ftc.gov/news-events/press-releases/2015/11/ftc-fcc-sign-memorandum-understanding-continued-cooperation.

Conclusion

Going forward, the FTC will continue its active privacy and data security enforcement, focusing on real consumer harms with the ultimate goal of making consumers better off. I hope that the FCC will use the same touchstone as it evaluates how to regulate broadband service providers' privacy and data security practices. Thank you for your attention, and I would be glad to take questions at this time.