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.

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

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 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/?321665-5/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 FTC has increased its privacy and data security enforcement.[9] Indeed, from the outside, it appears that the FTC'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.

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

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 60 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 *other* 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 is not 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—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 consumer's communications travels

[11] Fed. Comm. Comm'n, In the Matter of Cox Communications, Order and Consent Decree, DA 15-1241 (Nov. 5, 2015) [hereinafter Cox Order].

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 user's 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 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 access 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

In short,I believe there is little evidence

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.

FTC/FCC 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.

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.