United States of America

Federal Trade Commission

Remarks of Acting Chairman Maureen K. Ohlhausen[1]

Internet Privacy: Technology and Policy Developments

May 1, 2017

12:45 – 1:15PM

Rayburn Room 2044

Chris, thank you for that introduction, and hello to all of you. It's great to be here to talk about the interaction between privacy and technology and what that means for public policy. In particular, we're discussing those topics in the aftermath of the recent debate over the FCC's broadband privacy rules and the Congressional CRA that stopped them from taking effect.

These topics are at the core of the FTC's experience and expertise. Congress charged the Commission with the complementary but separate missions of promoting competition and protecting consumers. As part of our consumer protection mission, we are the primary U.S. privacy and data security enforcer and one of the most active privacy and data security enforcers in the world.[2] The FTC enforces a number of privacy and data security laws, including the Children's Online Privacy Protection Act and the Fair Credit Reporting Act. But our primary consumer protection enforcement authority is under Section 5 of the FTC Act, which prohibits

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.
[2] FTC Privacy & Data Security Update (2016), https://www.ftc.gov/reports/privacy-data-security-update-2016.

unfair and deceptive acts and practices in or affecting commerce. As the FTC has brought cases, we have developed precedent and guidance about what are unfair and deceptive practices across a wide variety of commercial areas. For more 20 years now, the FTC has applied its deception and unfairness authority to protect consumers' privacy. We have successfully brought more than 150 privacy and data security-related cases, including cases against some of the largest players on the Internet, including Google and Facebook. Perhaps as important – I don't like to count success merely by the number of cases – we actively educate business and consumers about privacy and data security risks. You can find those materials at ftc.gov.

The FTC also frequently brings together thought leaders and stakeholders to educate the Commission and to explore issues with future policy implications. We host workshops, some of which lead to reports or other guidance. Some of our recent technology-related workshops discussed the Internet of Things, big data, drones, FinTech and Artificial Intelligence. Coming up on June 28, we are cohosting with NHTSA a workshop on the privacy and data security issues for connected cars.[3]

Our flexible, enforcement-focused approach has enabled us to apply a consistent standard for consumer privacy across a wide range of changing technologies and business models. By focusing on practices that have already or are likely to harm consumers, we don't have to write prescriptive rules based on a guess about what harms might appear in the distant future – and in this fast changing world, five years is the distant future. Instead, our approach frees entrepreneurs to explore innovative business models and data uses, and we can focus on addressing any harms that develop.

[3] FTC, NHTSA to Conduct Workshop on June 28 on Privacy, Security Issues Related to Connected, Automated Vehicles (Mar. 20, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues.

So, with that background on the FTC's expertise, let me turn to the debate about ISP data collection and the latest developments. First, I'd like to put the whole matter into context. Part of that context is explaining that this debate about ISP data collection is not new. The FTC has explored this issue, and I'd like to tell you want we found. Finally, I'll address one potential area for Congress. And then I'd like to take your questions.

As you probably know, in October of 2016 the FCC adopted rules regulating privacy and data security practices of broadband internet access service providers, more commonly known as ISPs.[4] During the process leading up to this adoption, there was a lot of back and forth about the differences between the FCC and the FTC approaches. In fact, the FTC filed a unanimous, bipartisan comment stating that the FCC's approach was "not optimal," which was a very polite way of putting it. But in fact this collision between FCC and FTC was set into motion much, much earlier.

In fact, it goes back to the fall of 2014. That's when President Obama weighed in on the FCC's net neutrality proceeding in favor of reclassifying broadband as a Title II common carrier service. This put the FCC and FTC on a collision course.[5] Although the FTC has general jurisdiction, there are a few carve outs, including common carriers. Thus, if the FCC reclassified broadband as a common carrier service, it would elbow the FTC out of its long-standing authority to protect consumers in their interactions with their broadband providers.

I publicly warned of this "common carrier" collision course in the fall of 2014. But similar, bipartisan warnings go much further back. When I led the FTC's broadband internet

---

[4] FCC Adopts Broadband Consumer Privacy Rules (Oct. 27, 2016), https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules.

[5] November 2014: The President's message on net neutrality (Nov. 10, 2014), https://obamawhitehouse.archives.gov/net-neutrality#section-the-message.

access task force in 2006 and 2007, the experts we interviewed frequently emphasized the importance of retaining the FTC's jurisdiction over broadband providers. At that time, even the most vocal supporters of net neutrality regulation opposed Title II reclassification, in part because of the negative effect it would have on the FTC's consumer protection jurisdiction. You can read their concerns on pages 138-140 of the FTC task force's Broadband Connectivity Competition Policy report.[6] (As an aside, I am proud that the report remains an excellent introduction to the contours of the net neutrality debate. Of course, that also suggests we've been debating the exact same issues for ten years now without resolution.)

Anyhow, as I've mentioned, President Obama called for Title II reclassification in late 2014. And despite the long history of bipartisan warnings about the consumer protection effects of Title II reclassification, progressive supporters of net neutrality regulation didn't acknowledge the problem. In some cases, the same people who worried in 2007 that Title II would undermine consumer protections remained silent in 2015. In addition, many others who generally support the FTC's consumer protection efforts were apparently reluctant to oppose a plan endorsed by the President. Or perhaps they simply weren't aware of the problem. In any case, the FCC under the previous Chairman continued on this collision course, despite warnings.

And in 2015, the FCC proceeded to reclassify broadband as a common carrier service, pushing the FTC out of consumer protection of broadband subscribers.[7] This created a consumer protection gap, including a gap in consumers' privacy protections. A year and a half later, in

---

[6] FTC STAFF, BROADBAND CONNECTIVITY COMPETITION POLICY at 138-140 (June 2007), https://www.ftc.gov/reports/broadband-connectivity-competition-policy-staff-report.

[7] FCC Releases Open Internet Order (Mar. 12, 2015), https://www.fcc.gov/document/fcc-releases-open-internet-order.

October of 2016, the FCC adopted privacy rules for ISPs.[8] But those rules differed significantly from the FTC's approach to privacy. There were many differences between the approaches, but most problematically, the FCC rules defined "sensitive consumer personal information" much more broadly than does the FTC.

Now to get to the topic of this seminar! Advocates for the FCC privacy rules sometimes argue that the rules are essentially the same as FTC's approach.[9] But more often, they concede the difference and fall back to the alternative argument that different rules were appropriate because ISPs are uniquely situated to observe subscribers' data.[10]

But is this true? The FTC actually looked at this issue quite closely in the lead up to the FTC's latest comprehensive look at privacy, the 2012 Privacy Report.[11] The report found that ISPs have access to the unencrypted data that their customers send or receive, and therefore have the capability to develop detailed profiles of their subscribers.[12] But the report also concluded that ISPs were just one type of large platform provider with this kind of access.[13] Other platforms, such as operating systems, web browsers, search engines, and ad networks, raise very similar issues. The 2012 report therefore recommended that any privacy framework be

---

[8] *See supra* n.3.
[9] Terrell McSweeny, FCC should not leave broadband privacy rules to FTC (Mar. 5, 2017) ("As it turns out, there's not much difference at all … now the two agencies are using fundamentally the same approach."), http://thehill.com/blogs/pundits-blog/technology/322312-fcc-should-not-leave-broadband-privacy-rules-to-ftc.
[10] Frank Pallone Jr. and Terrell McSweeny, New Rules Intended to Protect Your Online Privacy Are Already Under Threat (Feb. 9, 2017) ("Some argue that the FCC's rules are unfair to internet service providers because platforms and websites are not under the same rules. … [But] Broadband providers potentially have access to every bit of data that flows from a consumer. That type of access demands a set of rules that matches the long held expectations of Americans…"), http://www.slate.com/articles/technology/future_tense/2017/02/consumer_privacy_rules_for_internet_service_providers_are_under_threat.html.
[11] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (Mar. 2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.
[12] *Id.* at 56.
[13] *Id.*

technology neutral – that is, that ISPs be treated like any other large platform.[14] Even though the report preceded my tenure at the Commission, I agree with its conclusion on this point.

Indeed, since that report was adopted in 2012, other major platforms have become much bigger and more capable of capturing consumer online activity. Recent research out of Princeton – and presented at the FTC's PrivacyCon this year – shows that the top online advertising company has trackers on more than 70% of the one million most popular websites.[15] That could facilitate a quite comprehensive view of online behavior. At the same, ISPs today are more constrained in what they can see, because more websites use HTTPS to encrypt the traffic between the website and the end user. As Google's latest Transparency Report states, "Secure web browsing through HTTPS is becoming the norm. Desktop users load more than half of the pages they view over HTTPS and spend two-thirds of their time on HTTPS pages."[16]

As a result, ISPs today are not particularly unique in either the volume or comprehensiveness of their ability to collect online information. Each type of platform has some data collection advantages and other disadvantages. Your home ISP can see traffic across that connection, but can't see your activities across your mobile carrier, office network, or coffee shop wifi. Your phone operating system can see any activity on your phone, but not on other devices. An ad network can see your browsing activity across websites, sometimes even on different devices, but only for websites where it has trackers. A search engine can aggregate your search history and clickthroughs, but only on that search engine. Your browser can see every website you visit – but you might use multiple browsers. Of course, certain companies

---

[14] *Id.*
[15] Steven Englehardt *et al.*, Insights from a 1-million-site Measurement of Online Tracking, slide 6 (Jan. 12, 2017), http://senglehardt.com/presentations/2017_01_ftc_online_tracking_insights.pdf.
[16] Google Transparency Report: HTTPS Usage (visited May 1, 2017), https://www.google.com/transparencyreport/https/metrics/?hl=en.

might have access to many or all of these types of information – but those companies generally aren't the major ISPs.

I'm sure the panel will dig much deeper into these technical issues. But the key takeaway is this: There isn't much evidence that ISPs have a uniquely pervasive view into user data that would justify government taking a privacy approach different from that applied to the rest of the Internet. That was the FTC's conclusion in 2012, and the support for a tech-neutral approach has only gotten stronger since then.

Before I conclude, and because I am speaking to a congressional audience, let me echo a long-standing, bipartisan FTC request. I mentioned earlier that the FCC's action in 2015 to reclassify broadband shoved the FTC out because our statute exempts common carriers from our general jurisdiction. That exemption is outdated. It was created more than a century ago when common carriers were pervasively regulated monopolies under price controls and other non-market constraints. Today, the market has changed. Telecom companies are now, competitively speaking, much more like the rest of the economy. And the current exemption no longer makes sense in today's environment where the lines between telecommunications and other services are increasingly becoming blurred. So I ask that Congress reform or repeal the exemption to ensure that the FTC can protect consumers everywhere on the Internet.

Thank you again for having me here today, and I'd be happy to take a few questions.