

DISSENTING STATEMENT OF COMMISSIONER AJIT PAI

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

For the last two decades, the United States has embraced a technology-neutral framework for online privacy. Administered by the Federal Trade Commission, this framework applied across all sectors of the online ecosystem. It reflected the uniform expectation of privacy that consumers have when they go online. It didn't matter whether an edge provider or ISP obtained your data. And it certainly didn't matter whether, as a consumer, you understood what those regulatory classifications meant—let alone the technical and legal intricacies that dictate when a single online company is operating in its capacity as an edge provider as opposed to an ISP. Regardless of all of that, the FTC's unified approach meant that you could rest assured knowing that a single and robust regulatory approach protected your online data.¹

That's why since the beginning of this proceeding, I have pushed for the Federal Communications Commission to parallel the FTC's framework as closely as possible. I agreed with my colleague that consumers have a "uniform expectation of privacy" and that the FCC thus "will not be regulating the edge providers differently" from ISPs.² I agreed that "consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected."³ I agreed that "harmonizing FCC policies with other federal authorities with responsibilities for privacy is a responsible course of action."⁴ And I agreed with the FTC when it said that an approach that imposes unique rules on ISPs that do not apply to all online actors that collect and use consumer data is "not optimal."⁵ These are the core principles that I have held throughout this proceeding.

I was disappointed—but not surprised—when FCC leadership circulated an *Order* that departed so dramatically from those principles. Over the past three weeks, my office diligently pursued a compromise framework that would have minimized the vast differences between the *Order*'s approach and the FTC's regime—one that would have protected consumer privacy while also allowing for more competition in the online advertising market, where edge providers are currently dominant.

For example, I asked my colleagues to acknowledge that persistent online identifiers (like static IP addresses) pose a larger privacy issue than more transitive identifiers. Distinguishing between the two in our de-identification standard would incentivize ISPs to compete with edge providers for online ads and do so through more privacy-protective technologies. Unfortunately, my colleagues were unwilling to compromise on this—or in any other meaningful respect.

¹ Indeed, the Obama Administration itself told the European Union that the FTC framework was strong and that nothing more, from a regulatory perspective, was needed to protect online consumers against predatory practices.

² Statement of Chairman Tom Wheeler, Hearing before the U.S. House of Representatives Subcommittee on Communications and Technology, "Oversight of the Federal Communications Commission," Preliminary Transcript at 141 (Nov. 17, 2015).

³ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2637 (2016) (Statement of Commissioner Jessica Rosenworcel).

⁴ Commissioner Jessica Rosenworcel Responses to Questions for the Record Submitted to the House Energy and Commerce Subcommittee on Communications and Technology's Hearing on "Oversight of the Federal Communications Commission" at 3 (July 12, 2016), available at <http://bit.ly/2eOhvkg>.

⁵ Federal Trade Commission Bureau of Consumer Protection Staff Comments at 8.

That leaves us with rules that radically depart from the FTC framework. And that leaves us with rules that apply very different regulatory regimes based on the identity of the online actor. As my colleagues' earlier comments make clear, as the FTC has made plain, this makes no sense.

Now, today's *Order* tries to justify this new and complex approach by arguing that ISPs and edge providers see vastly different amounts of your online data. It recounts what it says is a vast sea of data that ISPs obtain. It then says that "By contrast, edge providers only see a slice of any given consumers Internet traffic."⁶ A "slice." Really? The era of Big Data is here. The volume and extent of personal data that edge providers collect on a daily basis is staggering. But because the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a "slice" of consumers' online data. This is not data-driven decision-making, but corporate favoritism.

The reality—something today's *Order* does not acknowledge—is that edge providers do not just see a slice of your online data. Consider what the Electronic Privacy Information Center told us:

The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial threats for consumers are not the ISPs.⁷

Indeed, any review of the headlines rebuts the FCC's assertion that edge providers only see a fraction of your data. Consider these stories, almost all from just the past few weeks: "Google quietly updates privacy policy to drop ban on personally identifiable web tracking."⁸ "Privacy Debate Flares With Report About Yahoo Scanning Emails."⁹ "Apple keeps track of all the phone numbers you contact using iMessage."¹⁰ "Twitter location data reveals users' homes, workplaces."¹¹ "Amnesty International rates Microsoft's Skype among worst in privacy."¹²

But due to the FCC's action today, those who have more insight into consumer behavior (edge providers) will be subject to more lenient regulation than those who have less insight (ISPs). This doesn't make sense. And when you get past the headlines, slogans, and self-congratulations, this is the reality that Americans should remember: Nothing in these rules will stop edge providers from harvesting and monetizing your data, whether it's the websites you visit or the YouTube videos you watch or the emails you send or the search terms you enter on any of your devices.

So if the FCC truly believes that these new rules are necessary to protect consumer privacy, then the government now must move forward to ensure uniform regulation of all companies in the Internet ecosystem at the new baseline the FCC has set.

⁶ *Order* at para. 30.

⁷ EPIC Comments at 15.

⁸ Anmol Sachdeva, Google quietly updates privacy policy to drop ban on personally identifiable web tracking, *The Tech Portal* (Oct. 21, 2016), available at <http://bit.ly/2dIvcmY>.

⁹ Robert McMillan & Damian Paletta, Privacy Debate Flares With Report About Yahoo Scanning Emails, *Wall Street Journal* (Oct. 5, 2016), available at <http://on.wsj.com/2dI7ovW>.

¹⁰ Oscar Raymundo, Apple keeps track of all the phone numbers you contact using iMessage, *MacWorld* (Sept. 28, 2016), available at <http://bit.ly/2ev8QVi>.

¹¹ Patrick Nelson, Twitter location data reveals users' homes, workplaces, *NetworkWorld* (May 18, 2016), available at <http://bit.ly/1XmHAYf>.

¹² Dennis Bednarz, Amnesty International rates Microsoft's Skype among worst in privacy, *WinBeta* (Oct. 23, 2016), available at <http://bit.ly/2f8RnDv>.

That means the ball is now squarely in the FTC's court. The FTC could return us to a level playing field by changing its sensitivity-based approach to privacy to mirror the FCC's. No congressional action would be needed in order for the FTC to establish regulatory consistency and prevent consumer confusion.

Were it up to me, the FCC would have chosen a different path—one far less prescriptive and one consistent with two decades of privacy law and practice. The FCC should have restored the level playing field that once prevailed for all online actors using the FTC's framework. After all, as everyone acknowledges, consumers have a uniform expectation of privacy. They shouldn't have to be network engineers to understand who is collecting their data. And they shouldn't need law degrees to determine whether their information is protected.

But the agency has rejected that approach. Instead, it has adopted one-sided rules that will cement edge providers' dominance in the online advertising market and lead to consumer confusion about which online companies can and cannot use their data. I dissent.