Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

REPLY COMMENTS
OF
THE AMERICAN CIVIL LIBERTIES UNION ("ACLU")

Submitted: July 6, 2016

Reply Comments of the ACLU

The ACLU supports the proposal of the Federal Communications Commission (FCC or Commission) to apply the traditional privacy protections of the Communications Act to broadband Internet access service, and the ACLU submitted an initial comment supporting this proposed rulemaking on May 27, 2016. We write briefly to respond to the comments submitted by Professor Larry Tribe on behalf of CTIA, NCTA, and U.S. Telecom [hereinafter "Telecom comments"], which argue that the proposed rules violate the First Amendment to the U.S. Constitution. We disagree, and believe that the proposed rules are a necessary and tailored approach to protecting the privacy of the vast amounts of customer data created and stored by providers of Broadband Internet Access Service [BIAS].

As the Telecom comments discuss at length, it is true that recent court opinions have found corporate speech rights to be violated by the application of overbroad consumer protection and privacy laws. *See, e.g., Sorrell v. IMS Health*, 564 U.S. 552 (2011); *US West Communications, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999). But unlike those cases, the regulations at issue here directly and proportionally further a government interest of the highest order: ensuring that Americans can access the telecommunications infrastructure without having to trade away control over their most sensitive data.

The Telecom comments argue that in failing to bind other online entities (such as search engines, social media sites, and web browsers), the regulations unfairly and irrationally "single out" BIAS providers. But that is precisely backwards: the regulations' limited scope is evidence of their narrow tailoring, not evidence of selective enforcement. BIAS providers, which sit atop the Internet's backbone, have uniquely broad access to a wide swath of information about individuals' online activity, habits, purchases, and beliefs.

Following the Telecom comments' arguments to their logical conclusion, the government could never act to protect privacy unless it did so in a monolithic fashion, restricting every person who might arguably come into contact with personally identifiable information. But the cases cited by the Telecom comments do not support this argument, and such a rule would be a death knell to a number of widely accepted consumer protection laws.

Indeed, Congressional legislation frequently targets companies whose business model provides them central access to a customer's data. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710 (prohibiting video stores from disclosing customer information without consent); Driver's Privacy Protection Act, 18 U.S.C. §§ 2721 *et seq.* (restricting state motor vehicle departments and employees from disseminating motor vehicle records); Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d–2 *et seq* (restricting "covered entities" from releasing patient data without consent). That such laws do not also target other entities that come into contact with the exact same data—but whose general data collection does not create the same acute privacy risks—does not violate the First Amendment.

The ACLU strongly supports the Commission's proposal to apply the Communications Act's traditional privacy protections to BIAS providers. We believe that the proposed privacy protections are both constitutionally permissible and necessary to protect customers' privacy.

* * *

The Commission's proposal does not amount to an unconstitutional restriction of BIAS provider's commercial speech.

Because the regulations govern the use, sale, and disclosure of customer data (including to advertise additional products), they are subject to a form of intermediate judicial scrutiny used to assess commercial speech. *See, e.g., U.S. W., Inc. v. F.C.C.*, 182 F.3d 1224, 1232 (10th Cir. 1999). Under this analysis, the courts will consider whether the government's interest is *substantial*; if so, the regulation must then be *tailored* to directly advance that interest, with no more burden on speech than necessary. *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 566 (1980).

The Commission's proposal easily meets both tests.

The Commission has a substantial interest in protecting the private data of BIAS customers.

The proposed regulations cover not all online entities, but only BIAS providers, which operate as gatekeepers to the digital world. Notably, edge providers—such as websites, social media companies, and search engines—are not subject to the proposed rules. The Telecom comments argue that this defeats the government's interest in privacy. They are wrong.

As set forth in the ACLU's initial comments, the collection of information gleaned from the internet infrastructure itself (access to which is controlled by BIAS providers) poses distinct privacy concerns. BIAS providers can monitor not just a customer's visit to a single website, but

to all websites. Consumers also generally cannot simply avoid BIAS services since these providers control access to the telecommunications infrastructure that permits internet access, which is increasingly critical for individuals to work, access social services, and participate in society. . In addition, the lack of direct market competition among BIAS providers leads to significant market power. Even where equivalent competitive options are available, the switching costs can be considerable. Indeed, the oligopolic nature of the BIAS market is a critical justification for the FCC's underlying Open Internet Order and its constitutionality. In sum, consumers have far less market power in the single most important transaction required to access the Internet. BIAS providers simply should not have the additional power to manipulate prices or terms of service through use of customer data. Every use of customers' private identifying information should be expressly consensual, so that no customer of a necessary utility service need worry that they will be asked to trade their private info for online access. In today's world, digital access is a right, not a privilege to be riddled with conditions for access.

But it is not simply the market structure that justifies restrictions on the advertising power of BIAS providers. By their very nature—sitting on the backbone of the Internet, where they can monitor the entirety of customers' online traffic—they can create massive dossiers of human behavior that create a potential for unique privacy harms. The Supreme Court has recognized that this type of *cumulative* data about individuals, often enabled by digital technology, can create a privacy harm even where the discrete bits of data do not. For example, in *United States v. Jones*, 132 S. Ct. 964 (2012), five Justices recognized that long-term GPS location tracking violates an individual's reasonable expectation of privacy. And this is true even though "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." *Id.* at 964 (citing *United States v. Knotts*, 460 U.S. 276, 281–82 (1983)). In sum, the accumulation of many data points about an individual properly triggers the government's interest in protecting privacy.

The Commission has properly identified BIAS providers' unique role in both online access and data accumulation. There is thus no question that protection of the private communications data collected and stored by BIAS providers is of substantial government interest. *Cf., e.g.*, *Sorrell*, 131 S. Ct. at 2668 ("It may be assumed that, for many reasons, physicians have an interest in keeping their prescription decisions confidential."); *Bartnicki v. Vopper*, 532 U.S. at 532 ("Privacy of communication is an important interest."); *Alvarez*, 679 F.3d at 605 (same).

The Commission's proposed restrictions on the use and sale of customer data are tailored to furthering that interest.

The Commission has also decided that it has a substantial interest not only in preventing that *sale* of that customer data, but also any nonconsensual *use* of it. This is a proper and proportional approach to protecting the sanctity of common carriers upon whom we all rely to communicate with one another.

Once the government has established a substantial interest in empowering customers to control their personal data, it need not limit its protections to commercial sales of that data. Where the goal is to give each individual the ultimate say about how and when their personal information is used, a broad opt-in consent regime is the appropriate standard. The D.C. Circuit Court of

Appeals has examined another federal law's similar restrictions on the use of personal credit data—including a mandated opt-in consent regime—and found them to be constitutional:

> The harm that the Act and the Regulations are designed to prevent is not any specific **consequence** of the use and disclosure of consumers' nonpublic personal information; rather, **it is the use and disclosure of that information without the consent of the consumer**. Section 15 U.S.C. § 6801(a) makes this clear: "It is the policy of this Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." *Id.* Regulations prohibiting the use and disclosure of that information without the consent of the consumer clearly advance that interest. *United States v. Edge Broadcasting Co.*, 509 U.S. 418, 428, 113 S.Ct. 2696, 125 L.Ed.2d 345 (1993) (factual evidence unnecessary to establish that regulations directly and materially advance governmental interest where the link is obvious).

Individual Reference Servs. Grp., Inc. v. F.T.C., 145 F. Supp. 2d 6, 43 (D.D.C. 2001), *aff'd sub nom. Trans Union LLC v. F.T.C.*, 295 F.3d 42 (D.C. Cir. 2002) (emphasis added).

Here, the Commission has amply illustrated the substantial interest not only in preventing the sharing of customer data with outside entities, but in allowing individuals to maintain fundamental control over when and how their personal data is used. This is all the more important when BIAS providers have an unmatched ability to create intimate profiles of their customers activities and preferences; this comprehensive data should not be exploited for *any* purpose without a customer's consent—including profiling just to sell or advertise internal products.

The Telecom comments argue that, like the law in *Sorrell*, the proposed regulations are not tailored because they irrationally single out BIAS providers over other online actors. As explained above, BIAS providers are uniquely situated and are thus a proper target of regulation. Moreover, there is a fundamental difference between the proposed regulations and the Vermont law at issue in *Sorrell.* Regulations governing a certain industry (or type of data holder) are widespread and are not constitutionally suspect for that reason. *See, e.g.,* Video Privacy Protection Act, 18 U.S.C. § 2710 (prohibiting video stores from disclosing customer information without consent); Driver's Privacy Protection Act, 18 U.S.C. §§ 2721 *et seq.* (restricting state motor vehicle departments and employees from disseminating motor vehicle records); Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d–2 *et seq.* (restricting "covered entities" from releasing patient data without consent).

In *Sorrell*¸ by contrast, the law at issue prohibited the sharing of information based on the *content* of the data holder's speech. That is, the Vermont law allowed sale of the data to purchasers who wished to engage in certain educational communications, but strictly prohibited transfer of information to purchasers who would use the information for marketing. 131 S. Ct. at 2663. In other words, the statute "disfavor[ed] marketing, that is, speech with a particular content," and "disfavor[ed] certain speakers, namely pharmaceutical manufacturers." *See also Citizens United*, 558 U.S. at 340 ("Prohibited, too, are restrictions distinguishing among different speakers, allowing speech by some but not others. As instruments to censor, these categories are interrelated: Speech restrictions based on the identity of the speaker are all too often simply a

means to control content.") (citations omitted). *Sorrell* thus suggests that when a government acts to protect specific data, but distinguishes the level of protection for that same data based on the identity or motive of the speakers using it, the tailoring of the law is properly suspect.

What *Sorrell* absolutely does *not* hold is that privacy protections for certain kinds of *information,* or information stored or captured only by certain types of *entities*, are discriminatory. And the Commission's proposed regulations do precisely this: they restrain the use or sale of information stored by BIAS providers, who represent a unique threat to customer privacy. This is not a failure of tailoring that creates a First Amendment problem. And if it were, other laws that Americans rely upon to protect the privacy of their data would surely be at constitutional risk.

The Commission's proposal is similar to HIPAA, which the Supreme Court has distinguished as a targeted approach to protection of customer privacy.

There is at least one example of this kind of government regulation preventing the sale *or use* of customer data by companies who play a central role in creating or storing it: the Health Insurance Portability and Accountability Act [HIPAA]. Indeed, *Sorrell* – the case on which the Telecom comments predicate their constitutional objection -- specifically cites HIPAA as the paradigm of proper government regulation:

> For instance, the State might have advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances. See, *e.g.,* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d–2; 45 CFR pts. 160 and 164 (2010). A statute of that type would present quite a different case than the one presented here.

Sorrell v. IMS Health Inc., 564 U.S. 552, 573 (2011).

The telecom submission's fundamental complaint is that the Commission's proposal is under-inclusive because it regulates ISPs to the exclusion of edge providers. But in doing so, the proposal is essentially identical in structure to HIPAA.

Like the proposal, HIPAA regulates only those institutions that acquire protected information by virtue of unique access. HIPAA regulates, in effect, the ISPs of the health care system: health plans, health care clearinghouses, health care providers, and, in some cases, their business associates. *See* 45 C.F.R. § 160.102(a). But it does not regulate any of the numerous institutions and entities that do not fit within those terms' definitions but nonetheless have access to extremely private medical information. For example, it does not, as a general matter, cover: private genetic testing companies such as 23andMe; mobile-device manufacturers whose devices capture or store sensitive medical information; medical and fitness mobile-app providers; public agencies delivering social security or welfare benefits; health clinics that do not bill for services; most school health records; gyms and fitness clubs; health websites not offered by covered entities; many health researchers; nutritional counselors; commercial providers of personal health records; and many more.

And like the proposed regulations, HIPAA includes important exceptions even with respect to the entities it *does* regulate. For example, HIPAA generally regulates health care providers only

if they bill for their services electronically. And HIPAA includes a list of permitted disclosures, including, subject to certain criteria, those made to public health authorities, to employers, and to law enforcement, and those made to support health oversight activities, national security and intelligence activities, and protective services for the President.

In short, HIPAA and the proposal both regulate the primary point of contact that individuals have with, respectively, the health care system and the internet. The focus on BIAS providers and their unique control over customer data makes the proposed regulations properly tailored, not discriminatory.

Conclusion

The ACLU reiterates its support for the Commission's proposal. We believe that strong protections for the privacy of online users—who are required to share the most intimate details of their online lives with BIAS providers—represent a necessary, proportional, and constitutional use of the Commission's authority. We applaud the Commission for seeking to ensure that this powerful personal data is never used without users' consent.