THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY
ATTORNEY GENERAL

(617) 727-2200
(617) 727-4765 TTY
www.mass.gov/ago

Via Web Submission (ECFS)

October 19, 2016

Marlene H. Dortch, Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Comments on WC Docket No. 16-106: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

Dear Secretary Dortch:

Over the past few years, this Office has prioritized eliminating unfair or deceptive practices involving the collection, disclosure, and use of consumers' personal data. Our enforcement of the Massachusetts Data Protection Laws[1] has revealed that consumers face ever-increasing risks to the privacy and security of their sensitive personal information. We thus strongly support the Federal Communications Commission's proposed broadband Privacy Rule.[2]

Data breaches are a constant and increasing threat for companies and consumers alike, particularly with respect to information transmitted on the internet.[3] Consumers increasingly are also at risk of being denied credit, employment, housing, insurance, or other socioeconomic opportunities as their internet data feed algorithms that perpetuate socioeconomic, racial, or other

---

[1] Massachusetts Data Protection Laws require covered entities to develop, implement, and maintain minimum data security procedures and policies, consistent with industry standards, to safeguard Massachusetts consumers' "personal information" from unauthorized access or use, and to notify consumers in the event of a breach or compromise of that information. *See* Mass. Gen. Laws chapters 93H (Data Breach Notice Law), 93I (Data Disposal Law), and 201 C.M.R. 17.00 *et seq.* (Data Security Regulations).

[2] We support the rulemaking as initially proposed and as recently refined in the Fact Sheet released on October 6, 2016.

[3] From September 1, 2007 through December 31, 2015, this Office was notified of over 13,000 data breaches, over 3,000 of which occurred in 2015 alone.

disparities.[4]

As the gateways to the internet, broadband internet access service (BIAS) providers have unique access to the vast amounts of data that reflect consumers' daily personal, professional, and commercial affairs. Consumers cannot avoid BIAS providers or avoid sharing data with them. Nor can consumers readily change providers, given switching costs and limited provider options. Without any federal backstop of basic privacy protections, consumers have no meaningful knowledge, choice or control over what personal data their BIAS provider collects, what they do with that data, with whom they share it and for what reasons, or how it may be used against the consumer down the road. This status quo subjects consumers to unnecessary and unforeseeable risks, and threatens to erode the consumer trust critical to the internet economy.

We believe the Privacy Rule is a critical step towards protecting consumers' privacy online. The Privacy Rule sets forth clear and enforceable requirements that promote basic fairness and well-established principles of consumer choice, transparency, and security. In particular, we commend the Privacy Rule's requirement of express and affirmative consent (i.e., "opt in" consent) from consumers before BIAS providers may collect, use or disclose their "sensitive" personal information. The alternative – a negative option or "opt-out" mechanism – is fraught with the potential for unfairness or deception. BIAS providers should not be at liberty to exploit consumers' sensitive personal information unless and until consumers affirmatively opt out, especially where the consequences of not doing so are not clearly disclosed to the consumer in advance. To ensure that the "sensitive/non-sensitive" distinction furthers the goals of the Privacy Rule in the face of evolving technology and changing business practices, the FCC should consider building some flexibility into the definition of "sensitive" data for which opt-in consent is required.[5]

Likewise, consumers should not have to pay a premium to ensure their privacy or be forced to forego their privacy in order to obtain the important services that BIAS providers supply. We therefore also support the prohibition on "take it or leave it" offers, and heightened scrutiny for provisions that tie service price to privacy protections.[6]

---

[4] We highlighted such concerns to the U.S. Supreme Court in a recent amicus brief joined by twelve other States. *See* Brief of Amici Curiae States, *Spokeo, Inc. v. Robins et. al*., ___ U.S. __, 136 S. Ct. 1540 (May 24, 2016). There, we urged the Court to recognize the harm that consumers suffer when inaccurate information about them is harvested from the internet and used without their knowledge or control to determine their access to credit, job, housing, insurance, or other important socio-economic opportunities.

[5] As just one example, device identifiers – not defined as "sensitive" information under the current proposal – could be leveraged to generate a functional equivalent of a consumer's geolocation - which is considered "sensitive" under the Rule - as the consumer moves from his or her home computer, laptop, smartphone, and work computer throughout the day.

[6] October 6th "Fact Sheet" at 3.

Additionally, we urge the FCC to prohibit BIAS providers from compelling arbitration in their contracts with consumers. Our experience shows that pre-dispute mandatory arbitration clauses tend to benefit the party with more resources, often are presented in a manner that prevents consumers from understanding the adverse consequences on their legal rights, and prevents consumers from seeking redress through the judicial system. Such clauses erode the deterrent effect of the applicable consumer protection laws and leave consumers without effective redress.[7]

Finally, we believe that the FCC, with its jurisdictional authority drawn from a clear Congressional directive, is well-positioned to protect consumer privacy on telecommunications networks. Far from drawing arbitrary or artificial distinctions among the various participants in the internet ecosystem, the Privacy Rule's application to BIAS providers is a logical exercise of the FCC's enforcement mandate, and consistent with the status-based approach of other federal privacy regulatory schemes.[8] As the FCC has recognized, however, the State Attorneys General also play an active role in protecting their consumers' data privacy and security.[9] It thus is imperative that State Attorneys General continue to maintain their enforcement authority under their states' laws and that any preemption be as narrowly tailored as possible. To the extent some preemption is deemed necessary, we support the FCC's proposal to preempt state laws "only to the extent" they are inconsistent with the Privacy Rule's protections.[10] To allow the States to continue to protect their citizens in light of changing technologies and practices, we urge the FCC to articulate expressly within any enacted rule that its standards serve as a floor, and not a ceiling, or consumer protections.[11] *See, e.g.*, the Telephone Consumer Protection Act, 47 U.S.C. § 227(d) ("nothing in this section or in the regulations prescribed under this section shall preempt any State law that imposes more restrictive intrastate requirements or regulations on, or which prohibits" various enumerated activities).

---

[7] Attached is a letter to the Consumer Financial Protection Bureau from the Attorneys General of 18 States further describing the risks of pre-dispute mandatory arbitration clauses.

[8] *See, e.g.* Graham Leach Bliley Act, 15 U.S.C. §§ 6801–6809; 16 C.F.R. Parts 313 and 314 (federal standards applicable to financial institutions concerning the privacy and security of consumer financial information); the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191; 45 CFR Subpart C of Part 164 (federal standards applicable to health providers and other "covered entities concerning the privacy and security of personal health information); and the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) (federal law requiring federally-funded educational institutions to protect the privacy of student education records).

[9] Notice of Proposed Rulemaking at ¶ 276.

[10] *Id.*, ¶¶ 267-77.

[11] *See also* Truth in Lending Act, 15 U.S.C. § 1666j(a) ("The Bureau may not determine that any State law is inconsistent with any provision of this part if the Bureau determines that such law gives greater protection to the consumer); Equal Credit Opportunity Act, 12 C.F.R. § 1002.11 (a) ("A state law is not inconsistent if it is more protective of an applicant.").

Thank you for the opportunity to provide these comments with regard to the FCC's proposed Privacy Rule. We urge the FCC to move forward with its proposed rulemaking in order to provide consumers the robust privacy protections they deserve. Please do not hesitate to contact us with questions you may have about the points raised above, or about this issue in general.

Sincerely,

/s/ Sara Cable
Sara Cable
Director of Data Security & Privacy,
Assistant Attorney General
Consumer Protection Division

Encl.