STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE
BUREAU OF INTERNET
AND TECHNOLOGY

June 30, 2016

VIA WEB SUBMISSION AT <FCC.GOV/ECFS>

Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street NW
Washington, D.C. 20554

Re: Proceeding Number 16-106: Protecting the Privacy of Customers of Broadband and Other Telecommunications Service

Dear Chairman Wheeler:

The State Attorneys General ("State AG") are the chief law enforcement officers in their respective states. We have been granted broad authority to protect consumers and are especially concerned with matters related to consumer privacy. Our privacy laws protect consumers not only from identity theft, financial loss and other economic harms, but also from unauthorized disclosure or unfair use of more intimate details that could cause consumers public embarrassment, harassment or discrimination. Local knowledge, multi-state coordination and broad legal authority have allowed State AGs to effectively enforce privacy laws in the Internet age.

Against this backdrop, I write to express the support of the New York Attorney General's office ("NYAG") for the Federal Communications Commission's ("FCC") proposed rulemaking to establish privacy rules for Broadband Internet Access Service ("BIAS") providers. The proposed rule addresses an issue consumers rarely consider: the information BIAS providers collect about them. Consumers cannot avoid a BIAS provider the way consumers can avoid (without penalty), or otherwise freely and easily choose between, search engines or other

websites, or smartphone applications. Indeed, as the gateway to the Internet, BIAS providers are able to collect an unprecedented breadth of electronic personal information including not only a consumer's name, address and financial information but also every website he or she visited, the links clicked on those websites, geo-location information, and the content of electronic communications.

In 1996, Congress enacted Section 222 of the Communications Act, providing statutory protections to the privacy of the data that telecommunications carriers collect from their customers. The FCC now seeks to apply the privacy requirements of the Communications Act to BIAS and we fully support this effort. When consumers sign up for internet service, they should not have to sign away their right to privacy.

We support the FCC's broad definition of personally identifiable information ("PII"). The proposed rule appropriately extends PII beyond its historical conception as only those data elements identifying an individual (e.g. name, address, telephone number) to include information that is "linked or linkable" to a specific individual or device (e.g., IP address, MAC address). This definition is consistent with modern views of privacy in the Internet age and accounts for technological advancements that have enabled companies to link facially non-identifying data elements to customers or their devices.

The FCC proposes to protect consumer privacy using the three foundations of consumer privacy: transparency, choice and security. In particular:

1. Transparency: The proposal includes rules to enhance the ability of BIAS customers to make informed choices through effective disclosure of BIAS providers' privacy policies. These privacy policies include what customer information is collected, the purpose for such collection, what customer information is shared, with what entities said information is shared, and how, and to what extent, customers can opt-in or opt-out of such data collection and/or sharing. The proposal appropriately requires that BIAS providers give timely notice of their privacy policies to customers in "clear and conspicuous" and "comprehensible" language and make such notice persistently available and easily accessible on the provider's website and elsewhere.

We recommend that the FCC further require BIAS providers to make such privacy policies as concise as possible to increase the likelihood that customers will take the time to read and thereby comprehend them. We moreover recommend that the FCC require BIAS providers to use specific language, as opposed to vague statements, in their privacy policies so that customers can better understand the extent to which their data is collected, used, and shared. Finally, while we support the proposal's requirement that privacy notices be translated into each language that the BIAS provider previously used for any other notice, we recommend that the FCC extend this requirement beyond prior notices to cover all previous communications that the BIAS provider had with its customers, including advertising and sales. It would be unfair to customers to use their preferred language to persuade them to purchase a product, and then use a second language to provide critical information about the collection, use, and disclosure of their private information resulting from that purchase.

2. Choice: BIAS customers must have the ability to exercise meaningful and informed control over what personal data their BIAS provider collects, uses, and discloses and under what circumstances it shares their personal information with third parties. Ultimately, consumer choice turns on the context of the transaction and the consumer's existing relationship with the business.

The FCC's proposal recognizes that BIAS providers should have implied permission to collect, use, or share customer personal information as necessary to provide the contracted-for internet service. With respect to this implied permission, we recommend that the FCC require BIAS providers to contractually obligate all data recipients to limit their use of such data to the purposes enumerated in the proposed rule. The FCC's proposal affords customers an opt-out consent choice regarding the use of their data for purposes of marketing other communications-related services and sharing their data with the BIAS provider's affiliates. Finally, the FCC's proposal requires BIAS providers to secure opt-in consent from the customer before engaging in any other third-party commercial uses of the information. As recognized by the FCC's proposal, opt-in consent can only be obtained if (i) customers are presented with and have the ability to understand the full extent and consequences of what it is they are consenting to (i.e., merely checking a box indicating agreement with a terms of service and/or privacy policy would not constitute opt-in consent); (ii) consent is specific to the customer's information at issue; (iii) consent is voluntary and not conditioned in any way; and (iv) customers have the ability to easily revoke consent after opting-in.

We believe that the manner in which the privacy notice and opt-in or opt-out choice is presented to customers is critical to customers' ability to exercise their choice. Hence, we recommend that the FCC require BIAS providers to present customers with the privacy notice and choice option(s) upon initial login to the BIAS provider's website. The privacy notice and choice option(s) should be obvious to the user and presented in such a way as to not clutter the webpage and overwhelm the user. The objective should be to maximize the likelihood that customers will read and fully comprehend the privacy information. We also recommend that the FCC require BIAS providers to give customers the option to navigate to the privacy notice and choice option(s) upon all subsequent logins to the website so that customers can revisit the privacy notice and adjust their opt-in or opt-out settings. This navigation option should be displayed in an obvious location on the login landing page and the privacy content should only be located one click from the landing page. Finally, we recommend that, in the event of any changes to the BIAS providers' privacy policies and/or choice options, the FCC require BIAS providers to display an alert on the login landing page of their website notifying the user that there has been a change and directing the user to view the updated privacy information.

3. Security: The FCC's proposal requires that BIAS providers protect customer information that is stored or otherwise crosses their networks against unauthorized use or disclosure. The proposal requires data security practices that every BIAS provider must comply with, including risk management assessments, employee training, and corporate accountability. Consistent with our approach to data security, it is a technology-neutral, process-based approach to security that describes the steps a business should take to develop reasonable data security practices – with an emphasis on risk management – instead of enumerating particular technological measures.

The FCC's proposal requires BIAS providers to provide notice to affected customers within ten days after discovery of a breach of customer information and to the FCC within seven days after discovery of the breach. We recommend that, rather than using the proposed deadlines, the FCC consider a requirement that notice be provided "in the most expedient time possible and without unreasonable delay," the language found in most state data breach notice statutes, while also providing a final deadline "of not longer than" a fixed amount of time. Since the identification of the breached information and the customers associated with it can be a time consuming process, and certainly longer than the seven to ten days proposed, the FCC should consider adopting longer absolute deadlines. We moreover recommend that the FCC require BIAS providers to contractually obligate any affiliates or third parties to notify the BIAS provider in the event of a data breach so that the BIAS provider can then notify its customers.

However, BIAS providers should only be required to provide notice for a subset of PII. While we recognize that advances in computer science have demonstrated that seemingly anonymous information can be used to identify an individual, the proposed notification scheme presents real concerns over the value of its disclosure and presents risk of desensitizing customers to an increasing level of notification over exposed information.

The proposal defines "breach" broadly to include "any instance in which a person, without authorization or exceeding authorization, has gained access to, used or disclosed customer propriety information." While we have no objection to defining a breach broadly to include mere "access," as opposed to "acquisition" of the data, ultimately the breadth of this definition must be measured against the scope of the data elements that trigger notification, and the appropriate balance must be reached. While not addressed by the proposal, we would like to see the FCC post on its website the data breach notices it receives, consistent with the Department of Health and Human Services Office for Civil Rights practice for protected health information breach notices, pursuant to Section 13402(e)(4) of the HITECH Act.

As State AGs, we are active participants in ensuring our citizens have robust privacy protections and we feel that it is critical that we continue this work. Thus, we understand that, consistent with the FCC's approach to the current Section 222 rules, states can continue to craft, administer and enforce laws regarding the collection, use, disclosure, and security of customer data that are more restrictive than those adopted by the FCC, provided that BIAS providers are able to comply with both federal and state laws, and preemption would only apply to directly inconsistent state laws on a case-by-case basis, without the presumption that more restrictive state requirements are inconsistent with these rules. If a BIAS provider can comply with both state and federal law, they should have to.

In our digital, interconnected world, protecting consumer privacy is essential. Consumer online information is easily collected, and behavior is easily tracked, especially by those that provide the gateway to the internet. There is a need for enhanced regulation in this area. As these new technologies emerge, concerns regarding online privacy will become even more prevalent and it is imperative that the FCC and the states maintain broad authority for privacy regulation and enforcement.

We support your proposal, and in your rulemaking we strongly urge you to put the consumer first and maximize consumer choice.

Sincerely,

Kathleen McGee
Bureau Chief
Bureau of Internet and Technology