Received & Inspected
AUG 30 2016
FCC Mail Room

COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL
HARRISBURG, PA. 17120

Bruce L. Castor, Jr.
Cell: 717-497-4789
E-mail: bcastor@attorneygeneral.gov

August 23, 2016

The Honorable Tom Wheeler
Chairman of the Federal Communications Commission
445 12th Street NW
Washington, DC 20554

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

Dear Chairman Wheeler:

As chief legal officers charged with protecting consumers and citizens in our respective states, we write to urge you to reconsider the approach to internet privacy reflected in the proposed rules under consideration in this docket.

As more and more of our commercial, cultural, and social lives migrate online, protecting digital privacy has never been more vital. But no matter how well intentioned, rules that do not reflect the online experience and expectations of ordinary consumers will only confuse the public and undermines users' privacy interests.

The core problem with the Commission's proposal is that it would arbitrarily create two different sets of rules to govern the same data being used for the same purposes by competing Internet-based companies and platforms.

This inconsistency runs counter to years of guidance on privacy from the White House, the Federal Trade Commission, and your agency calling for one harmonized, consistent set of guidelines.[1] And it will not benefit consumers, 94% of whom believe "All companies

---

[1] See, e.g., Protecting Consumer Privacy in an Era of Rapid Change, FTC Report, Federal Trade Commission, at 56 (Mar. 2012) ("Any privacy framework should be technology neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity."); Executive Office of the President, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, White House Report, at 36 (Feb. 2012) (calling for "a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions."); *Continued Oversight of the FCC: Hearing Before the Subcomm. on Communications & Technology of the House Energy and Commerce Comm.*,114th Cong., Transcript at 107-108 (2015) (Statement of Tom Wheeler, Chairman, FCC) ("we work closely with the FTC[;] we will do our best to harmonize so that there is a com mon set of concepts that govern privacy.").

collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it."[2] These principles are reflected in the FTC comments submitted in this docket, which question the patchwork approach.[3]

It also runs counter to logic and marketplace facts. All of us are familiar with the vast world of free or low-cost products and innovative services that depend on analysis of consumer data for their vitality.

Recognizing these benefits to innovation, competition, and investment, the FTC and the Administration have consistently endorsed a technology-neutral regulatory approach, treating apps providers, platform providers, broad band providers, and other internet-based companies the same. Yet you have proposed to reject that well-established and successful approach for internet providers, potentially stifling innovation and depriving broad band consumers of these benefits.

Your office and our colleagues in New York who support this bifurcated approach claim it is needed because internet providers have heightened access to data because they are "gateways" to the online world. But while this point has intuitive appeal, it is not supported by the facts. The latest research by well-respected privacy expert Peter Swire shows that, because nearly 70% of online data will be encrypted by the end of this year and because consumers use multiple different internet services in one day (home, work, mobile, public hotspot), broad band providers do not have any heightened access to consumer data.[4] In fact, it is apps, platform providers, edge services, operating systems, device ecosystems, and others that track us from device to device and computer to computer and know the most about where we go, what we do, and who we are online. As Swire concludes, "based on a factual analysis of today's Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts."[5]

We also share the FTC's concern about you r decision to base privacy protection on who is using data as opposed to the sensitivity of the information itself. Under your rules, the same opt-in consent requirement applies both to routine public or mundane information such as IP addresses and to highly sensitive data such as medical or financial data. As the FTC explained, this approach "does not reflect the different expectations and concerns that consumers have for

---

[2] Comments of Progressive Policy Institute (May 2016).
[3] FTC Staff Comments (May 2016).
[4] Peter Swire, Justin Hemmings, & Alana Kirkland, *Online Privacy and ISPs; ISP Access to Consumer Data is Limited and Often Less than Access by Others,* Working Paper of the Institute for Information Security & Privacy at Georgia Tech, at 3-4 (Feb. 29, 2016),), http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.
[5] *Id.*

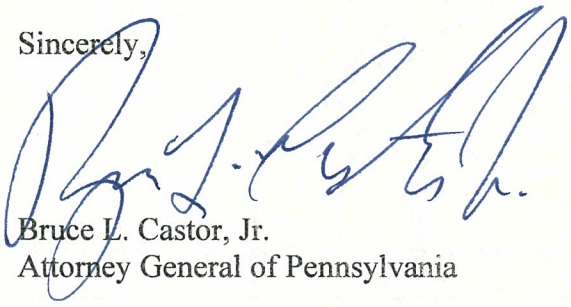
sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful."[6]

That is not what consumers assume will happen - in a recent survey, 83% believed that online privacy protection should be based on the sensitivity of data, not on who is collecting and using it.[7] And it will distort markets by arbitrarily burdening some market participants while leaving others comparatively unchecked - something especially troubling from a competition perspective as the large tech firms continue to grow, consolidate, and dominate more and more platforms and markets. So we agree with the FTC's recommendation to apply an opt-in consent requirement solely to sensitive information and to recognize that "[o]pt-out is sufficient for use and sharing of non-sensitive data."[8]

We understand that jurisdictional issues make it difficult for the FCC alone to promulgate consistent harmonized privacy regulations for the entire internet ecosystem. As state Attorneys General, we deal with that problem every day - issues outside our formal jurisdiction routinely affect our communities, our citizens, and our local economies.

But from our perspective, the only way to resolve such problems is through collaboration and cooperation - working with peer agencies and jurisdictions to develop an effective harmonized approach for all entities. Unilateral action can be satisfying and politically popular, but it rarely solves problems - and often creates new ones of its own.

Sincerely,



Bruce L. Castor, Jr.
Attorney General of Pennsylvania

BLC/mc

---

[6] FTC Comments at 22.
[7] PII Comments.
[8] FTC Comments at 20, 35.