Testimony of Nancy Libin

On Behalf of NCTA – The Internet and Television Association

on

LD 946 – An Act to Protect the Privacy of Online Customer Information

April 24, 2019

Chairman Lawrence, Chairman Berry, and distinguished Members of the Committee on Energy, Utilities and Technology:

Thank you for the opportunity to submit this testimony regarding legislation introduced before this committee, L.D. 946, An Act to Protect the Privacy of Online Customer Information.

My name is Nancy Libin, and I am a partner at the law firm of Davis Wright Tremaine LLP, where I co-chair the Privacy, Security and Technology practice. Prior to private practice, I served from 2009 to 2012 as the Chief Privacy Officer of the U.S. Department of Justice ("DOJ"), where I was the DOJ representative to the Obama White House's interagency task force that developed the Obama Administration's approach to consumer data privacy.

I am here today on behalf of NCTA – The Internet & Television Association, the principal trade association for the U.S. broadband and pay television industries. NCTA commends the Committee for its attention to this very important issue. The challenges facing consumers' privacy are growing, and we support efforts to address them. We are concerned about L.D. 946, however, because it diverges from the widely adopted and well-established approach that the Obama Administration and Federal Trade Commission ("FTC") developed to respond to these challenges. While well-intentioned, L.D. 946's divergent approach would have serious unintended consequences, failing to meaningfully protect—and even frustrating—Maine consumers and imposing requirements that would be impossible for companies to meet.

Consumers expect and benefit from a consistent privacy regime that protects their personal information regardless of who is collecting it.[1] The FTC's technology-neutral approach

---

[1] *See* Memorandum from Public Opinion Strategies and Peter D. Hart to the Progressive Policy Institute, Key Findings from Recent National Survey of Internet Users (May 26, 2016) (showing that 94 percent of consumers favor such a consistent and technology-neutral privacy regime, i.e., they overwhelmingly want the same privacy protections to apply to their personal information *regardless* of the entity that collects such information) available at

to privacy regulation[2] and the framework adopted in the Obama Administration's 2012 Privacy Report ("Obama Privacy Report")[3] do just that. The FTC spent months examining companies' practices, even holding a public workshop examining the practices of broadband providers, and it concluded that there was no need to single out broadband providers for heightened restrictions.[4] The European Union's General Data Protection Regulation ("GDPR"), which is widely regarded as the most rigorous privacy regime in the world, similarly applies to all commercial entities doing business in Europe that collect, use, and share personal information. All of these regimes reflect the reality of the 21st century Internet economy by regulating the same data consistently across the digital ecosystem, regardless of the nature of the entity involved.

L.D. 946 takes a starkly different approach. It heavily regulates a single group of companies in the online data services ecosystem—providers of "broadband Internet access service," which have had a strong track record in protecting consumer privacy—[5] but leaves edge providers—including search engines, social networks, mobile apps, and other large platform providers—regulated under the FTC's flexible framework, and it would not apply to companies,

---

https://www.progressivepolicy.org/wpcontent/ uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf.

[2] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012) ("FTC Report") at 15 (stating that the framework applies to "all commercial entities that collet or use consumer data"), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[3] 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* (February 2012) ("Obama Privacy Report") at 10 (stating that the framework applies to all "commercial uses of personal data"), available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

[4] FTC, *The Big Picture: Comprehensive Online Data Collection* (2012), available at https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection.

[5] In a January 2019 report, the Government Accountability Office identified 101 privacy-related enforcement actions by the FTC in the past decade, ***only one of which involved an ISP***. *See* Government Accountability Office, Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility (Jan. 2019) at 21, available at https://www.gao.gov/assets/700/696437.pdf.

such as third-party data brokers that collect personal information about consumers but do not have any direct relationship with consumers. But ISPs, at best, have fractured and variable access to the typical Internet user's daily activity. Academic research and empirical studies show that certain technologies—such as encryption and Virtual Private Networks—substantially limit ISPs' visibility into users' online activity and are widely available and increasingly used.[6] Moreover, the typical Internet user accesses the Internet through multiple devices, some of which are mobile, and connects to the Internet through various ISPs and Wi-Fi networks at any given time throughout the day.[7] This shift to mobile and multiple devices, however, has not hampered edge providers' ability to continue to collect, use, and share more, and a wider variety of, data about users. By narrowly focusing on ISPs, L.D. 946 fails to protect consumers in the areas where their privacy is most at risk.

Nor does the bill explain how consumers will be protected if their personal information is disclosed to third parties (with the required opt-in consent) who mishandle their information, as was the case, for example, in the Cambridge Analytica situation that spawned much concern about these issues.[8] Indeed, many of the data privacy and security incidents reported over the last

---

[6] *See, e.g.,* Peter Swire, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less Than Access by Others,* February 29, 2016, ("Swire Report") available at http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf ("We present new evidence about the rapid shift to encryption, such as the HTTPS version of the basic web protocol. Today, all of the top 10 web sites either encrypt by default or upon user log-in, as do 42 of the top 50 sites. ... An estimated 70 percent of traffic will be encrypted by the end of 2016. Encryption such as HTTPS blocks ISPs from having the ability to see users' content and detailed URLs. There clearly can be no "comprehensive" ISP visibility into user activity when ISPs are blocked from a growing majority of user activity."); Liam Tung, *"Google: This surge in Chrome HTTPS traffic shows how much safer you now are online,"* ZDNet.com, Oct. 23, 2017, available at https://www.zdnet.com/article/google-this-surge-in-chrome-https-traffic-shows-how-much-safer-you-now-are-online/ ("The percentage of HTTPS page loads on Chrome is growing on all platforms. HTTPS traffic on Android is now 64 percent compared with 42 percent a year ago. HTTPS-protected traffic on Chrome for Mac and ChromeOS is 75 percent, up from 60 percent and 67 percent respectively a year ago. Google also notes that 71 of the 100 most popular sites have now enabled HTTPS by default, up from 37 a year ago."). More recently, Google's Transparency Report shows that 93 percent of all the pages loaded on the Chrome platform are encrypted by HTTPS as of March 30, 2019. *See* Google Transparency Report, https://transparencyreport.google.com/https/overview?hl=en (Last visited April 19, 2019).

[7] Swire Report at 24-25.

year have been caused by such third parties. The bill's failure to even address this set of issues illustrates that this legislation does not fully protect consumers.

In addition to covering *all* entities and addressing the obligations of third parties, the Obama Administration and FTC privacy frameworks ensured that companies were permitted to use data to engage in legitimate business activities, innovate, and adapt to ever-changing technology. They achieve this important balance by focusing on actual privacy harms to consumers and subjecting *sensitive* data to heightened protection through opt-in consent, while allowing greater flexibility to use and share *non-sensitive* data and enabling entities to use and disclose data when consistent with the context of the relationship between the consumer and the company and within consumers' expectations.[9]

Drawing on these principles, the FTC established tiers of consumer choice that allow companies to infer consent for practices that are consistent with the context of the consumer's relationship to the company; provide an opt-out mechanism when the context does not permit consent to be inferred; and recommend opt-in consent only in limited circumstances, such as when companies deliberately collect and market using sensitive data.[10] The Obama Administration took the same context-driven approach, recognizing that consent could be inferred for certain uses and disclosures of data. The Obama Privacy Report explained, for instance, that companies could "infer consent to use and disclose personal data to achieve objectives that consumers have specifically requested, as long as there is a common understanding of the service," to "conduct marketing in the context of most first-party relationships, given the

---

[8] Kathleen Chaykowski, *Lawmakers Grill Facebook on Privacy Practices, Pitfalls of Ad-Fueled Business,* Forbes (Apr. 10, 2018), available at https://www.forbes.com/sites/kathleenchaykowski/2018/04/10/lawmakers-grill-facebook-on-privacy-practices-pitfalls-of-ad-fueled-business/#21ee1a433705.

[9] FTC Report at 36-44; 47-48

[10] *Id.*

familiarity of this activity," and to use personal data for purposes that are "common," such as "analyzing how consumers use a service in order to improve it, ... complying with ... legal obligations, and protecting intellectual property."[11]

L.D. 946, on the other hand, would require companies to obtain opt-in consent from consumers, subject to overly narrow exceptions, before companies use, disclose or make available to any person a broad range of information. As written, the bill would not even allow a broadband provider to use information about customers' use of broadband services for well-recognized internal business purposes, such as improving the services or developing new products and services, without *opt-in* consent. And it would not allow a broadband provider to use such information to protect its networks and provide a secure online environment for its customers – something customers not only expect, but demand from their providers. These results are even more bizarre when one considers that every other entity on the Internet will be able to use the same information for these same purposes without opt-in consent. These marketplace-distorting results may not be intended, but nonetheless this is how the bill currently reads.

Moreover, L.D. 946's advertising and marketing exception allows broadband providers to market only their own "communications-related services" – a term that the bill does not define, but that likely excludes pro-consumer Internet of Things devices and services, such as home security and other innovative services that some broadband providers increasingly are offering. This restriction, too, departs from the FTC's approach, which allows companies to infer consent for most first-party marketing, recommends that companies provide consumers with an *opt-out* mechanism when the context of marketing does not allow consent to be inferred, and recommends *opt-in* consent only in certain, very limited circumstances, such as when companies deliberately

---

[11] Obama Privacy Report at 17.

collect and market using sensitive data.[12] The FTC's approach has protected consumers while allowing innovation and economic growth in the Internet economy. L.D. 946, however, would prevent broadband providers from adopting this business model, while allowing other online entities to continue doing so. The bill also goes far beyond not only the FTC's framework, but even the 2016 Federal Communications Commission ("FCC") broadband privacy order, which allowed ISPs to engage in all first-party marketing based on non-sensitive personal information subject to *opt-out* consent.

Even more problematic, the bill violates the First Amendment of the U.S. Constitution. It is well established that the First Amendment protects companies' ability to communicate with existing and potential customers, and rules that single out and restrict one class of speakers – such as ISPs – are subject to heightened scrutiny. L.D. 946 does precisely that. It imposes unique, discriminatory restrictions on ISPs' ability to engage in commercial speech while leaving other entities that use the exact same information in the same medium for the same purposes free to continue to engage in such speech. The U.S. Supreme Court held in *Sorrell v. IMS Health Inc.*, that such discriminatory speaker-based restrictions violate the First Amendment.[13] Complicating matters further, the bill defines "customer personal information" without distinguishing between sensitive data (e.g., social security numbers; health, financial, or children's information; or precise geolocation data) and non-sensitive data (e.g., names, addresses, demographic data, and device identifiers). Yet, not all data, even if misused or wrongfully disclosed, has the same potential to harm consumers. For that reason, the FTC carved out five categories of data that it deemed particularly sensitive and in need of heightened protection such as opt-in consent.[14] The GDPR

---

[12] FTC Report at 40-41; 57-60.

[13] 131 S. Ct. 2653.

and the California Consumer Privacy Act also distinguish between these two types of personal information and apply more restrictions to sensitive data.

Moreover, L.D. 946's definition of "customer personal information" is overbroad and lacks any limiting principle. It includes two categories: (1) "personally identifying information about a customer, including but not limited to the customer's name, billing information" and so forth, and (2) "information from a customer's use of broadband Internet access service, including but not limited to" web browsing history, app usage history, device identifiers, as well as other listed and unlisted information.[15] The bill does not require information in category (1) to be paired with information from category (2), or for information in category (2) to be linked or linkable to an identified individual, as is typically the case in privacy laws. Thus any "information from a customer's use of broadband Internet access service"—regardless of whether it is connected to an *identifiable* or even a *specific* or *particular* individual—would be subject to the bill's prohibitions. The bill would potentially capture virtually all data that broadband subscribers generate when they use broadband services, regardless of whether it has been de-identified, anonymized, or aggregated, prohibiting broadband providers from using, disclosing or making such information available unless the provider obtains the customer's prior consent or can satisfy the narrow requirements of the bill's limited exceptions. This sweeping definition will impede providers' ability to conduct business and network operations and substantially degrade the Internet experiences of customers in Maine, without providing any meaningful benefit to consumers because every other company on the Internet already has access to, collects, and/or uses this information.

---

[14] The FTC identified the following categories of data as sensitive: children's information, financial information, health-related data, social security numbers, and precise geolocation information. FTC Report at 59.

[15] L.D. 946, § 9301(C)(1), (2).

These technical infirmities also make other features of L.D. 946 unworkable. For example, the bill prohibits broadband providers from making consent to the disclosure of personal information a condition of "serv[ing]" the customer. The bill does not indicate whether it prohibits such conditions only in connection with providing broadband Internet access service or in connection with providing any service that a provider may offer. Either way, it will not be possible for providers to function if they have to provide certain services to consumers who refuse to consent to the disclosure of their personal information necessary to facilitate such services in the first place.

The bill also prohibits offering customers a discount for agreeing to provide consent. This goes far beyond, and will cause more harm than, the similar controversial provision in the California Privacy Protection Act. It would prohibit – without exception – companies from providing discounted services, loyalty programs, and other financial incentives, such as access to content in exchange for receiving targeted advertising. Provided that the terms of the exchange are clear, there is no privacy benefit to be gained by prohibiting this exchange, and it will only serve to diminish consumers' online experience and access to price discounts and other benefits. Even the GDPR provides consumers greater choice by allowing companies to offer ad-supported content in exchange for consumers' consent to receive online ads.[16]

In addition, the bill allows consumers to prohibit providers' use of information that is not "customer personal information." It is not clear what such information would be, but in any event, this provision serves no consumer protection purpose and would interfere with a host of operations online that consumers expect to be executed quickly and without service interruption. For instance, this provision could affect providers' ability to share information necessary to

[16] Regulation (EU) 2016/697 of the European Parliament and of the Council, Art. 7 (Apr. 27, 2016), available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

enable the transmission of data across networks. ISPs simply will not be able to comply with this provision and continue to provide service.

In addition, the bill applies not to citizens or residents of Maine, but to the personal information of *any* customers who happen to be "located" in Maine while using broadband service on a mobile device and are billed for that service in the state, even if the individual resides in another state. In many circumstances, it will not be possible for a provider to know where a customer is located without collecting addition information about the precise geolocation of every individual with which it interacts. As such, the extraterritorial application of the bill would undermine the key goal of *protecting* consumers' privacy by forcing broadband providers to track the movements and locations of all customers at every moment in time. And yet, the bill requires providers to obtain express affirmative consent from customers before using precise geolocation information for any purpose other than those listed in the exceptions, which do not include determining a customer's location for purposes of compliance with the bill. Surely, that cannot be the intent of the bill, yet that is how it currently reads. And if such precise location information cannot be obtained by the business, compliance will be impossible.

Finally, the bill is unnecessary. The FCC has repealed its 2015 Open Internet Order that reclassified ISPs as common carriers, and ISPs are once again under the FTC's jurisdiction. FTC Chairman Simons made that clear last month when he said that the FTC stands ready to "challenge deceptive and unfair privacy and security practices by ISPs."[17] Moreover, the Maine attorney general and Maine consumers already have the ability to hold broadband providers accountable for unfair and deceptive acts or practices—including failing to adhere to

[17] Remarks of Federal Trade Commission Chairman Joseph Simons, Free State Foundation Speech at Eleventh Annual Telecom Policy Conference (Mar. 26, 2019) available at https://www.ftc.gov/system/files/documents/public_statements/1508991/free_state_foundation_speech_march_26.pdf

representations they have made about their privacy practices or maintain reasonable data security safeguards—under the Maine Unfair Trade Practices Act.[18]

In sum, the Committee should be commended for raising this important issue. In its current form, however, L.D. 946 would have many unintended consequences that would not serve—and would in fact, harm—the interests of Maine consumers. Internet privacy is a complicated issue that transcends industries, business models, and state borders. For that reason, NCTA and its members are strong supporters of a national privacy framework. Indeed, we are working with federal legislators to help them develop robust federal privacy legislation. Two years ago, federal privacy legislation was improbable. But now, there is bipartisan consensus in Congress and across all industry sectors for such legislation. We encourage the Committee to work with Members of Congress on both sides of the aisle who are actively engaged in developing a strong federal privacy bill. We therefore respectfully urge the Committee to hold the bill and see how Congress proceeds this year with federal legislation.

Thank you again for the opportunity to appear before you today.

---

[18] Me. Rev. Stat. Ann. tit. 5 § 207.