ACLU
AMERICAN CIVIL LIBERTIES UNION
Maine

121 Middle Street, Suite 200
Portland, ME 04101
(207) 774-5444
www.aclumaine.org

TESTIMONY OF OAMSHRI AMARASINGHAM, Esq.

LD 946 - Ought To Pass

An Act to Protect Privacy of Online Customer Personal Information

JOINT STANDING COMMITTEE ON ENERGY, UTILITIES AND TECHNOLOGY

April 24, 2019

Senator Lawrence, Representative Berry, and members of the Committee on Energy, Utilities and Technology, greetings. My name is Oami Amarasingham, and I am the advocacy director for the American Civil Liberties Union of Maine, a statewide organization committed to advancing and preserving civil liberties guaranteed by the Maine and U.S. Constitutions. On behalf of our members, we ask you to vote "ought to pass" on LD 946.

Background on FCC regulations

In 2016, the Federal Communications Commission (FCC) implemented long-awaited regulations establishing basic privacy rules pertaining to internet service providers' (ISP) collection, use, and sale of sensitive customer information. The regulations aimed to protect internet users' private information much in the same way federal regulations have long protected the privacy of landline phone users.

Just as telecommunications regulations bar AT&T and other telephone service providers from gleaning information about us from our phone calls and monetizing that information, the FCC regulations barred internet service providers, or "ISPs"[1] from collecting, using, or monetizing sensitive customer information without opt-in consent from the consumer.

In 2017, Congress used a seldom-used law, the Congressional Review Act, to overturn the FCC regulations.

Neither the FCC nor the FTC can Act to Protect Consumer Privacy

Unfortunately for consumers, the Congressional Review Act contains a provision barring regulatory agencies from ever instituting "substantially similar" regulations if the Act is used to eradicate them. It will therefore be difficult—and may require a change to the Congressional Review Act—for the FCC to institute regulations to protect internet users under a future administration.

[1] ISPs are also sometimes referred to as broadband internet access services ("BIAS").

Nor can the Federal Trade Commission (FTC) act to protect consumer privacy. While the Ninth Circuit recently ruled that the FTC retains some jurisdiction of ISPs, the FTC's powers are *remedial* powers. The FTC can only vindicate consumer rights after there has been an unfair and deceptive trade practice. Thus the FTC does not provide adequate protection for two reasons: first, the FTC can only act after the harm has been done, which may provide closure for consumers, but does not undo the harm; second, ISPs can get around the FTC by simply disclosing their practices to consumers, who have no real choice but to take whatever conditions an ISP wants to put on their contract. In addition, the FTC lacks rulemaking authority, and so could not promulgate privacy regulations similar to the now-repealed FCC regulations. Instead, the FTC can only step in to hold ISPs accountable for violating consumer rights *after* those violations have occurred and the damage has been done.

Key Components of LD 946

Because neither the FCC nor the FTC can enact privacy protections for consumers, state legislatures across the country are considering legislation to provide consumers with protections similar to the repealed FCC regulation under state law. LD 946 is a strong step towards regaining what Maine consumers lost when Congress eliminated the federal privacy regulations. Among the key elements in LD 946 are:

- Definitions of "customer personal information." Any legislation that aims to provide Mainers with FCC regulation-equivalent protections must clearly stipulate what information is protected by the law. Crucially, LD 946 identifies location information, communications content, web browsing information, application usage history, and health and financial information as "personal" and therefore subject to opt-in requirements.

- A ban on the use, disclosure or sale of customer personal information absent the granting of customer opt-in approval, with few exceptions. The exceptions in LD 946 are comprehensive, and allow for the provision of internet service, billing, customer-requested service assistance, and emergencies.

- A requirement that the opt-in process and language be "clear and conspicuous." In other words, it's important that ISPs don't hide the truth about what they want to do with our information in fine, legalistic print that many people will not read or understand. LD 946 stipulates that information about the opt-in process be written and presented in ways that will provide maximum benefit to the public.

- A ban on "Pay-for-Privacy" and other incentives for customer opt-ins, and prohibition from providing different qualities of internet service to customers based on their opt-in status. This is essential to prevent companies from undermining the intent of the law. Some companies, including AT&T, have already experimented with Pay-for-Privacy schemes, charging substantially less

money to people who allow the company to sell their sensitive information.[2] It isn't fair to grant privacy rights only to those who can afford them. Nor is it acceptable for companies to provide privacy-conscious customers with lesser quality service.

LD 946 is not Preempted by Federal Law

In general, federal privacy protections are considered a floor, not a ceiling. States are free to enact stronger privacy protections – and Maine has a long history of doing just that.

While only a court could definitively rule on preemption, we do not believe that LD 946 would be preempted by federal law. Under the Supremacy Clause, federal laws and regulations may, in some circumstances, preempt state laws and regulations. There are three general types of preemption: (1) express preemption; (2) field preemption; and (3) conflict preemption. Express preemption applies where a federal law or regulation explicitly states that it preempts state law. *See Cipollone v. Liggett Group, Inc.*, 505 U.S. 504, 516 (1992). Field preemption applies where a federal law wholly occupies a given area of law, to the exclusion of all state law. *Id.* Conflict preemption applies where federal law and state impose conflicting obligations such that compliance with both is impossible ("impossibility preemption"), or where state law poses an obstacle to the accomplishment and execution of a federal law's purposes and objectives ("obstacle preemption"). *See Fidelity Federal Sav. & Loan Ass'n v. de la Cuesta*, 458 U.S. 141, 153 (1982). There is a "presumption against preemption," but this presumption does not apply in areas of law that have traditionally been subject to federal regulation. *See Buckman Co. v. Plaintiffs' Legal Comm.*, 531 U.S. 341, 347 (2001).

Nor does express preemption apply here, because the relevant federal statute regulating privacy of telecommunications customer information, Section 222 of the Communications Act, is silent with respect to preemption. *See* 47 U.S.C. § 222. Field preemption also does not apply here, because the FCC has consistently ruled that Section 222 does not preempt all state laws governing customer proprietary network information (CPNI). Rather, the FCC has said that it will determine whether its regulations preempt state laws on a case-by-case basis, depending primarily on whether those laws impose irreconcilably conflict with its regulations, without imposing any presumption that more stringent state privacy protections are preempted by federal law or FCC regulations.[3]

---

[2] Sandra Fulton, "Pay-for-Privacy Schemes Put the Most Vulnerable Americans at Risk," Free Press, May 10, 2016. Available at https://www.freepress.net/blog/2016/05/10/pay-privacy-schemes-put-most-vulnerable-americans-risk.

[3] *See* Federal Communications Commission, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended; 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers, Third Report and Order and Third Further Notice of Proposed Rulemaking*, 17 FCC Rcd 14860, 14891–93 (2002) (2002 CPNI Order); Federal Communications Commission, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking*, 22 FCC Rcd 6927, 6958 (2007) (2007 CPNI Order).

Because the bill's provisions are based on the FCC's repealed broadband privacy order, and the federal law in this area has not changed since 2017, LD 946's provisions are fully consistent with existing federal law and FCC regulations.

We do not believe that LD 946 runs afoul of the Dormant Commerce Clause doctrine, which prohibits states from imposing inappropriate burdens on interstate commerce. First, LD 946 does not violate the extraterritoriality doctrine. Under that doctrine, laws that regulate purely out-of-state transactions are invalid. Here, however, LD 946 regulates ISP interactions only with respect to their in-state consumers. It is presumably feasible for ISPs to identify these individuals and implement appropriate safeguards for their protected information.

LD 946 does not violate the *Pike* balancing test. Under that test, state laws that impose indirect burdens on interstate commerce are invalid if those burdens are disproportionate to the law's legitimate local benefits. *See, e.g., Brown-Forman Distillers Corp. v. New York State Liquor Auth.*, 476 U.S. 573, 579 (1986). Like many state laws, LD 946 may impose some burdens on interstate commerce by regulating the commercial activities of national and international corporations, but these burdens are justified by the significant privacy benefits afforded to Mainers.

Finally, LD 946 does not threaten to expose ISPs to conflicting duties. *See, e.g., Bibb v. Navajo Freight Lines*, 359 U.S. 520 (1959) (striking down an Illinois law that required trucks to use contoured mudguards while driving on in-state highways, because the law conflicted with other states' mudguard requirements). We have heard arguments that a patchwork of laws across the country will be unworkable for ISPs. However, it seems plausible that ISPs could tailor their practices for consumers in each state to conform to that state's privacy protections. While an ISP might have economic incentives to apply a national policy that conforms with even the most stringent state privacy protections, that alone does not suffice to make out a Dormant Commerce Clause violation. *See, e.g., Nat'l Federation of the Blind v. Target Corp.*, 452 F. Supp. 2d 946, 961 (N.D. Cal. 2006) ("Courts have held that when a defendant chooses to manufacture one product for a nationwide market, rather than target its products to comply with state laws, defendant's choice does not implicate the commerce clause." (collecting cases)).

The Maine Legislature Must Act Because the Market Will Not Provide Adequate Privacy Protections

We are skeptical that the market will provide meaningful privacy protections for the average consumer. Most Mainers do not have a choice between multiple providers for access to high speed internet. In many parts of the state, there is only one ISP who can deliver high speed internet, making it impossible for Mainers to choose a provider with strong privacy policies. While it is true that consumers can take some steps to protect their privacy, it is unrealistic to expect the average Maine consumer to have a sophisticated knowledge of encryption or virtual private networks (VPNs). And indeed, many websites and streaming services do not work if a consumer is using a VPN or ad-blocker in an effort to protect their privacy. Moreover, investing in VPNs and other

privacy protections is expensive. Without privacy protections that apply to all consumers, only those few consumers with the tech savvy and financial means to buy privacy will be entitled to it.

Unregulated, your ISP will know you better than you know yourself—and they will be able to sell all the detailed sensitive information they collect about you to other companies or the government, which will be able to use it in ways you will never fully understand. Indeed, as artificial intelligence systems become more intelligent and complex, enabling new forms of surveillance, tracking, and data analytics, the stakes for establishing commonsense internet consumer privacy couldn't be higher. Information collected by ISPs and sold to the highest bidder can be used to swing elections, alter individual lives, manipulate public discourse, and even populate FBI databases. If state legislatures don't protect internet consumer privacy, people in America will not be able to use the internet without subjecting themselves to increasingly dangerous levels of unregulated corporate and government surveillance.

Federal privacy protections are a floor, not a ceiling. In other words, the states have the right to enact legislation that further protects the privacy of its citizens. And the Maine legislature has done this many times. In the 1970s when wiretapping was the cutting edge technology, Maine banned the practice almost entirely. More recently, recognizing the federal government's failure to update laws ensuring cell phone privacy, Maine passed landmark legislation to protect the privacy of all cell phone users in Maine.

We cannot look to Washington D.C. to fix a problem it is responsible for creating. The burden of ensuring that Maine consumer privacy rights are protected therefore falls to this body. We urge the committee to vote "ought to pass" on LD 946.