Harold "Trey" L. Stewart III
Senator, District 2
Senate Republican Leader

THE MAINE SENATE
131st Legislature

3 State House Station
Augusta, Maine 04333

LD 1284, "An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information"

Joint Standing Committee on Judiciary

May 5, 2025

Senator Carney, Representative Kuhn and Distinguished Members of the Joint Standing Committee on Judiciary:

I am Trey Stewart; and I represent Senate District 2, which includes several communities in Penobscot and Aroostook Counties. I am here today to present LD 1284, "An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information."

I want to begin by making one thing clear: this is not an effort to undo privacy protections for Mainers. Quite the opposite. This is about updating and strengthening our approach to privacy to reflect the world we actually live in today.

In 2019, Maine passed a law that applied only to internet service providers (ISPs). At the time, that may have seemed like a step forward; but today, we know that protecting privacy means protecting data, no matter who handles it. Limiting our focus to just one type of company doesn't reflect how personal information is actually collected, used, or shared in the modern digital marketplace.

This legislation is about fairness, consistency, and effectiveness. It treats ISPs the same as every other business that interacts with personal data – from search engines to online retailers to mobile apps. Passing comprehensive privacy alongside this bill will make sure that Mainers still have strong protections and clear rights.

Privacy should not be a partisan issue. It's a consumer issue; and Maine has the opportunity to join the growing number of states across the country that have already taken action – states that have declined to focus on single types of entities and instead passed comprehensive privacy frameworks that focus on the data itself. We can protect Mainers' personal information while still ensuring that Maine businesses can operate and compete in a modern, global economy on equal footing.

Having a law in Maine that imposes privacy restrictions on Internet Service Providers alone created a moral hazard for consumers and for legislators. For consumers, the 2019 law implies that their personal information is protected when they go online. Most consumers are not going to dive deep into the nuances of a law we pass when deciding whether and how to protect their information online. So, it is entirely reasonable and expected that consumers understood the passage of 2019's Act To Protect the Privacy of Online Customer Information as, in fact, protecting the privacy of their information online.

But the law didn't do that then, and it doesn't do that now. It singles out one type of company – ISPs – as the problem while ignoring the dozens of other companies that handle the exact same personal data.

Take a man in Maine who's researching options for VA benefits and mental health support after military service. He may believe he's protected under Maine's 2019 law because he didn't opt in to data sharing with his internet provider; but then he starts seeing ads for therapy services, military-related pharmaceuticals, and insurance policies tailored to veterans. How did that happen?

Because the law only stops ISPs from using or selling that data. It says nothing about the search engine he used, the health site he visited, or the analytics firm tracking every click. His personal information was never really protected because the law focused on who had the data, not what the data was.

Mainers want privacy that travels with their data – no matter who's handling it. A law that only applies to one stop on the information highway doesn't deliver that. It's a false sense of security and Mainers deserve better.

Even the focus on ISPs is misplaced. When this law was passed and in comments since that time, advocates for the law have claimed that ISPs occupy a special position with respect to their visibility into consumer data. But this was not true in 2019 and becomes less true each year as more data is encrypted online. Nearly 90% of websites are encrypted using https and all major browsers will alert users if they are visiting an unencrypted site. Even Mozilla notes that this encryption prevents ISPs from seeing anything that a user does on a website or anything beyond the top-level name of the site. So, an ISP can see their subscriber visited https... maine.gov but not what they entered into the search box or that they visited the subpage for adoption services; however, maine.gov knows what they searched for and visited, as does every advertiser or other website that is tracking them across the internet.

ISPs don't have some special window into our personal emails. Like most websites these days, email services use encryption, which scrambles the information while it's being sent. That means ISPs can't see the contents of our emails or the specific pages we visit. At most, they can see things like the name of the website we're connecting to, how long the connection lasts, and how much data gets used. That's the same kind of basic connection info that the email company or website itself can see.

It's also important to understand that email providers have access to more detailed information about what you're doing on their platforms. They can read your messages, scan content for advertising purposes, and track activity. ISPs don't have that kind of access. So even when an ISP also offers an email service, it's not getting more insight than any third-party email provider. And if people are still worried about what their ISP might see, there are easy tools they can use, such as VPNs, which basically create a secure tunnel between your device and the internet. Once a VPN is turned on, the ISP can't see anything beyond the fact that you're connected to the VPN. There are also alternative DNS services that handle your web address lookups separately from your ISP, giving users even more privacy options.

At the end of the day, it's clear that ISPs aren't uniquely positioned to invade our privacy; and, in some cases, they have less access to personal data than the platforms we actually use every day. These are the situations for which Mainers are demanding protection – protection from being tracked, protection from unknown entities receiving their data, protection from their data being sold, protection from their personal information being used in ways that they don't expect and don't consent to. The ISP law fails to provide any of these protections, while implying it does so. That is a real harm to Mainers.

For legislators, this law has created our own moral hazard. We have spent the last several years failing to meaningfully protect our constituents' privacy while patting ourselves on the back for a job well done. It is telling that of the almost 20 states to have adopted consumer privacy laws, none have followed Maine's lead of focusing on internet service providers only; and each includes a broad base of entities that collect or have access to data, which includes internet service providers. I am not saying that ISPs should not be included in privacy protections. That is not the reason for this bill to repeal the 2019 law. Instead, everyone – including them – should be regulated the same and have obligations to consumers. All other states' privacy laws are designed to protect consumers' personal information no matter which entity gets its hands on it. Repealing our current law and pivoting to that approach is the best way to protect Mainers. We cannot solve this problem by ignoring our existing law while adopting a comprehensive privacy law on top of it. Doing so would still leave Maine with a regime focused on entities rather than consumers and their personal information. No consumers, or at best very few, will understand that a social media company, a search engine, or an AI chatbot has different requirements for handling their personal information than their ISP, which may require different forms of consent. The simplest and clearest way to protect consumers is to adopt consistent laws that reflect their expectations and desires.

It's also worth remembering that when Maine passed the 2019 ISP-only privacy law, it was heard in the Energy, Utilities and Technology Committee – not Judiciary. That made sense at the time because the bill was narrowly focused on internet service providers. But look where we are now. Today, all comprehensive privacy legislation, including the bills before us, is rightly being considered by the Judiciary Committee. That's not a small shift. It reflects a broader and more accurate understanding of privacy in the modern world.

Privacy today is no longer just a technology or telecom issue. It's a legal issue, a civil rights issue, and a consumer protection issue. The fact that the Legislature itself has recognized this complexity is a signal that we can no longer afford to treat privacy as if it starts and ends with ISPs. It doesn't – and Mainers know it.

Unlike every comprehensive state consumer privacy law, Maine's existing ISP-only privacy law lacks both the right to delete and the right to correct; but we have those rights. We should exercise them by deleting 2019's too-narrow ISP law and correcting course by adopting comprehensive consumer privacy legislation.

Thank you for your time and consideration.