TESTIMONY REGARDING L.D. 1284
"AN ACT TO REPEAL PROVISIONS OF LAW GOVERNING THE PRIVACY OF BROADBAND INTERNET CUSTOMER PERSONAL INFORMATION"

BEFORE THE MAINE SENATE'S COMMITTEE ON JUDICIARY

By Michael J. Santorelli, Director
The Advanced Communications Law & Policy Institute
New York Law School

May 5, 2025

* * * * * *

Executive Summary

The ACLP at New York Law School supports L.D. 1284 and makes the following points in support of its passage:

1. Maine's current ISP-focused data privacy law does not reflect the realities of the digital ecosystem or the harms that stem from it.
2. In the absence of strong, comprehensive, and uniform data privacy laws – and without policymakers willing to stand up to rapacious data harvesters – firms for which data is their lifeblood will continue unabashed in their pursuit of more and more of our sensitive information.
3. The harms of unrestrained data collection and monetization practices by tech firms are becoming more visceral by the day, with children and teens bearing the brunt of ever more intrusive harvesting techniques.
4. The inadequacy of Maine's digital privacy framework is also evident by simply comparing the current law, which applies only to ISPs, and the proposed comprehensive data privacy laws also pending before the Committee today. The roster of proposed protections in the comprehensive bills are not currently available to the people of Maine, leaving them exposed to myriad potential harms.
5. Repealing the ISP-focused privacy law is a necessary first steps towards bolstering online protections in Maine.

* * * * * *

Thank you for the opportunity to offer testimony today.

My name is Michael Santorelli. I am the director of the Advanced Communications Law & Policy Institute (ACLP) at New York Law School.[1] The ACLP monitors, writes about, and regularly weighs in on broadband and tech-related policy developments across the country. The ACLP has long been a vocal advocate for strong, comprehensive, and uniform data privacy laws, which are needed to protect consumers from having their sensitive online information harvested and monetized without their knowledge or consent.[2] Without clear rules of the road, online companies whose business models rely on the monetization of personal data will continue to do as they please in the digital Wild West.

In this testimony, the ACLP makes five points in support of L.D. 1284, passage of which would signal that Maine takes seriously the gravity of the issues before it.

First, Maine's current data privacy law, which L.D. 1284 seeks to repeal, does not reflect the realities of the digital ecosystem or the harms that stem from it.

Let's follow the money.

The current law only covers ISPs and does not address the behavior or reflect the business models of any other actor in the digital ecosystem. ISPs make almost all their money from selling broadband, video, and voice services to customers. For all other actors in the digital ecosystem – edge companies; data brokers; AI firms; etc. – data monetization is their lifeblood. As such, these firms are constantly figuring out new and more intrusive ways of getting increasingly granular data about us and our online habits so they can make more money.

Consider Meta. In 2024, nearly 98% of Meta's $164 billion in revenues stemmed from advertising.[3] For the uninitiated, it might seem like Meta's Facebook is the primary source of data fueling its advertising revenue since that is where people voluntarily post a lot of personal information. However, over the years, it has come to light that Facebook represents the tip of a massive iceberg of murky data collection practices by Meta. Indeed, in its pursuit of market share and financial growth, Meta has created an endless array of methods for gathering data from consumers. Every few years, a new data collection scandal implicating a previously unknown data collection technique by Meta comes to light and horrifies the public.[4]

This dynamic is not unique to Meta. Rather, it is emblematic of the financial incentives that drive almost all non-ISP firms in the digital ecosystem. Remember: if something is free (e.g., email, social media, search, etc.), then you are the product.

Second, in the absence of strong data privacy laws – and without policymakers willing to stand up to rapacious data harvesters – tech firms will continue unabashed in their pursuit of more and more of our sensitive information.

Without strong privacy laws that apply equally to all digital firms, there is a real likelihood that data collection and monetization could become even more intrusive and pernicious as firms race to become leaders in AI. This is not a hypothetical. The next data harvesting onslaught involves integrating AI into a host of products, including wearable tech like glasses, watches, and even neural implants, so that they can collect data from us wherever we are.[5] AI feeds on data, and those training AI tools have shown little regard for IP laws or privacy norms.[6]

In the age of AI, treating ISPs as the primary privacy menace makes no sense.

Third, the harms of unrestrained data monetization practices by tech firms are becoming more visceral by the day. Unbridled data collection creates a toxic feedback loop that allows tech companies to make their offerings even more addictive. This is especially harmful to children and teens, who, unfortunately, are bearing the brunt of the myriad negative outcomes of this addiction.

These harms are also evident in the increasing politicization of tech firms and the weaponization of the data they collect. In the last few years, there have been many instances of states using digital data to track people and arrest them if they search for the "wrong" thing.[7] At the same time, the leaders of many of these firms have demonstrated time and again how craven they are to remain among the richest people in the world by kowtowing to those in elected office.[8] What's to stop them from handing over user data in exchange for, say, laxer antitrust enforcement?[9]

Fourth, the inadequacy of Maine's privacy framework to protect consumers' data is also evident by simply comparing the current law, which applies only to ISPs, and the proposed comprehensive data privacy laws also pending before the Committee today. Indeed, the proposed comprehensive laws offer a compelling inventory of all the protections that the people of Maine currently lack vis-à-vis voracious tech companies. Without laws that articulate users' rights in their data, prohibit pernicious data collection activities, offer specific protections for children, and include mechanisms to opt out of data collection, the people of Maine remain at the mercy of tech companies, who have demonstrated that they have little regard for how their data collection practices impact the people they rely on to stay in business.

Fifth, repealing the current law is a necessary first step towards assuring comprehensive data privacy in Maine.

Repealing the current law will not change the status quo because, as discussed above, the ISP-focused law does nothing to protect consumers from the bad behavior of other actors in the digital ecosystem. Moreover, repeal is necessary to pave the way for the adoption of a comprehensive privacy law, which will provide a more uniform approach to privacy protection. A law that applies equally to all actors in the digital ecosystem will enhance personal protections and provide much-needed consistency across the online experience,

more so if that law is also consistent with the comprehensive privacy laws already adopted in almost 20 states. The people of Maine will be certain that, no matter what kind of online activity in which they engage or which service provider they use (ISP, social media app, search engine, etc.), their rights and protections will not change.

In conclusion, the ACLP supports passage of L.D. 1284 and encourages the state to embrace stronger, more comprehensive, and more uniform data privacy laws. Doing so will bolster protections for the people of Maine and signal to the states that have yet to adopt these laws that this is a path worth following.

Thank you again for the opportunity to testify.

Notes & Sources

[1] For additional information, please visit www.nyls.edu/aclp and www.broadbandexpanded.com.

[2] Link to 2016 FCC Filing: http://comms.nyls.edu/ACLP/ACLP-Privacy-Comments-WC-Docket-No-16-106-052716.pdf; Link to 2018 NTIA Filing: http://comms.nyls.edu/ACLP/ACLP-Comment-to-NTIA-Docket-No.-180821780-8780-01-November-9-2018.pdf.

[3] *Meta Reports Fourth Quarter and Full Year 2024 Results,* Jan. 29, 2025, Meta, https://investor.atmeta.com/investor-news/press-release-details/2025/Meta-Reports-Fourth-Quarter-and-Full-Year-2024-Results/default.aspx.

[4] *See, e.g.,* Michael Santorelli, *Halo, Goodbye: Cleaning up the Digital Ecosystem After the Facebook Data Spill*, April 24, 2018, Forbes, https://www.forbes.com/sites/washingtonbytes/2018/04/24/halo-goodbye-cleaning-up-the-digital-ecosystem-after-the-facebook-data-spill/; Todd Feathers et al., *Facebook is Receiving Sensitive Medical Information from Hospital Websites,* June 16, 2022, The Markup, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites; Sara Morrison, *Meta is Getting Data About you From Some Surprising Places,* June 17, 2022, https://www.vox.com/recode/23172691/meta-tracking-privacy-hospitals; Anna Cooban, *Meta Accused of 'Massive, Illegal' Data Processing by European Consumer Groups,* Feb. 29, 2024, CNN, https://www.cnn.com/2024/02/29/tech/meta-data-processing-europe-gdpr/index.html; Lena Cohen, *Mad at Meta? Don't Let Them Collect and Monetize Your Personal Data,* Jan. 17, 2025, EFF, https://www.eff.org/deeplinks/2025/01/mad-meta-dont-let-them-collect-and-monetize-your-personal-data.

[5] *See, e.g.,* Kyle Barr, *Meta Will Reportedly Flood the Market With AI Wearables in 'Year of Greatness,'* Feb. 6, 2025, Gizmodo, https://gizmodo.com/meta-will-reportedly-flood-the-market-with-ai-wearables-in-year-of-greatness-2000560206.

[6] *See, e.g.,* Gil Appel et al., *Generative AI Has an Intellectual Property Problem,* April 7, 2023, Harvard Business Review, https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem; Isabel Gottlieb and Cassandre Coyer, *AI's Data Appetite is Huge. That's a Problem for Privacy Laws,* July 24, 2024, Bloomberg, https://news.bloomberglaw.com/artificial-intelligence/ais-data-appetite-is-huge-thats-a-problem-for-privacy-laws.

[7] *See, e.g.,* Cat Zakrzewski et al., *Texts, Web Searches About Abortion Have Been Used to Prosecute Women,* July 3, 2022, Wash. Post, https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/.

[8] *See, e.g.,* Jessica Karl, *Amazon Doesn't Want You To Know How Much the Trade War Costs,* April 29, 2025, Bloomberg, https://www.bloomberg.com/opinion/newsletters/2025-04-29/amazon-should-show-tariff-price-increases-despite-trump-bezos-call.

[9] *See, e.g.,* Julia Shapero, *Big Tech Struggles to Find Footing in Trump's First 100 Days,* May 1, 2025, The Hill, https://thehill.com/policy/technology/5273502-big-tech-struggles-to-find-footing-in-trumps-first-100-days/.