ACLU
AMERICAN CIVIL LIBERTIES UNION
Maine

PO Box 7860
Portland, ME 04112

(207) 774-5444
ACLUMaine.org
@ACLUMaine

TESTIMONY OF ALICIA REA, ESQ.

LD 1822 – Ought to Pass
An Act to Enact the Maine Online Data Privacy Act

LDs 1224, 1088, 1284 – Ought Not to Pass
An Act to Comprehensively Protect Consumer Privacy
An Act to Enact the Maine Consumer Data Privacy Act
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, greetings. My name is Alicia Rea and I am a policy fellow at the ACLU 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, I urge you to support LD 1822 and oppose LDs 1224, 1088, and 1284.

Privacy and Bodily Autonomy

The rights to privacy and bodily autonomy are at the core of access to abortion and gender affirming health care. Throughout the country, our bodies have become battlegrounds on these fronts. Privacy and bodily autonomy connect several issues, from abortion and contraception to gender-affirming care and marriage equality. These are all linked by our foundational right to life, liberty and the pursuit of happiness. These rights and freedoms allow us to write our own stories, determine our own paths, and thrive on our terms.

Following the United States Supreme Court's opinion overturning *Roe v. Wade*, questions and fears about our digital privacy and the criminalization of healthcare have proliferated.[1] The criminalization of people seeking reproductive health care, and of doctors and nurses who seek to provide it, has expanded since this decision, with out-of-state actors seeking information about Maine patients and providers who engage in healthcare that is legal in this state. In the face of these attacks on reproductive healthcare and other care that is legal in Maine, our digital privacy matters even more today than it has in the past.

[1] *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 (2022).

The lack of strong digital privacy protections has profound implications in the face of expanded criminalization of reproductive and gender affirming health care. The recent breathtaking and authoritarian attacks on bodily autonomy mean that we must fight with new urgency to ensure that people maintain control over their personal information. If we fail, the repressive surveillance techniques and powers that police and prosecutors have used to wage the ineffectual and damaging wars on drugs and terror will be marshaled to track, catalogue, and criminalize patients and those seeking basic information about health issues.

Laws that criminalize reproductive health and gender affirming care are already being used disproportionately by government actors to surveil, penalize, and control people, especially people of color. According to Pregnancy Justice, the past 15 years have seen a shocking spike in arrests and prosecutions for crimes related to stillbirths, miscarriages, and alleged drug and alcohol use during pregnancy.[2] Of the 1,792 people prosecuted for these offenses since 1980, 1,379 were charged after 2006, and those targeted were disproportionately Black and Indigenous women.[3] And, just last year, U.S. Senator Ron Wyden, revealed that an anti-abortion political group used mobile phone location data to send targeted misinformation to people who visited any of 600 reproductive health clinics in 48 states.[4]

Prior to the *Dobbs* decision, a Texas district attorney and sheriff worked to indict and arrest a 26-year-old woman and charge her with murder, after the woman self-managed her abortion.[5] In 2017, an online search for the abortion medication misoprostol was used to charge one woman with second-degree murder.[6] In 2015, a series of text messages with a friend about getting an abortion helped convict another woman of feticide and child neglect.[7]

Expanded criminalization of healthcare has become increasingly common, which is why we must be prepared to digitally defend ourselves against

---

[2] Pregnancy Justice, *The Rise of Pregnancy Criminalization*, Sep. 2023, available at https://www.pregnancyjusticeus.org/wp-content/uploads/2023/09/9-2023-Criminalization-report.pdf.
[3] *Id.*
[4] Letter from U.S. Senator Ron Wyden to FTC Chair Lina Khan and SEC Chair Gary Gensler (Feb. 13, 2024), available at https://www.wyden.senate.gov/imo/media/doc/signed_near_letter_to_ftc_and_sec.pdf.
[5] Nicole Narea, *Why was a Texas woman charged with murder over an abortion?*, Vox, available at https://www.vox.com/policy-and-politics/23021104/texas-abortion-murder-charge-starr-county.
[6] Cat Zakrzewski et al., *Texts, Web Searches About Abortion Have Been Used to Prosecute Women*, The Washington Post (July 2022), available at https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/.
[7] Emily Bazelon, *Purvi Patel Could Be Just the Beginning*, New York Times (Apr. 2015), available at https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html.

ACLU
AMERICAN CIVIL LIBERTIES UNION
Maine

corporate and government surveillance. We must take real action to protect our digital privacy, in the face of attempts to invade Maine's current legal protections.

Over the past 20 years, digital technologies have rapidly advanced, changing the way we communicate, seek and share information, travel, work, play, document and track our own health metrics, find love, and more. Billion-dollar industries have taken shape that work behind the scenes and without consent to create, share, trade, and sell extremely sensitive data about hundreds of millions of people, buoyed by leaps in computing power and the declining cost of data storage.

The Government can gain access to this corporate surveillance in what some have called a "public-private surveillance partnership." In many cases, government actors can obtain extremely detailed information from corporations about people's finances, internet use, and communications without ever going to a judge, and without a shred of evidence that someone is involved in criminal activity. When cops are armed with court orders, virtually none of the information collected and processed in what has been called the "surveillance capitalist" marketplace is off limits to the government. And even for types of personal information that courts have said police can only force companies to turn over with a warrant—like cell phone location data—government agencies are sidestepping the warrant requirement by paying to access sensitive information instead of going to a judge. The Fourth Amendment should not be for sale, yet our inadvertent transfer of our sensitive data to private companies means there can be no expectation of privacy in the data collected, stored, and sold.

A lack of local-related data privacy can also have serious implications for one's livelihood. In 2001, "[t]he top administrator of the U.S. Conference of Catholic Bishops resigned after a Catholic media site told the conference it had access to cellphone data that appeared to show he was a regular user of Grindr, the queer dating app, and frequented gay bars."[8]

In response to these profound transformations, civil rights advocates have championed consumer privacy protections to give people control over their personal information. In Illinois, such protections limit what kinds of information companies can collect and the ways they can share and use these

[8] Michelle Boorstein et al., *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, Wash. Post (July 21, 2021), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.

ACLU
AMERICAN CIVIL LIBERTIES UNION
Maine

data.[9] In Virginia, the state legislature passed a law that prohibits the collection, use, or sharing of reproductive or sexual health information without consent and provides Virginians with a private right of action for at least $500 per violation..[10]

Legislatures must impose strict limitations on the use of invasive technologies and techniques, restricting surveillance warrants to only the most serious kinds of criminal investigations and excluding investigations related to sexual health and gender affirming care. Maine should seek to preserve access to healthcare for all Mainers by taking extreme care to protect information created or maintained in our jurisdiction from being disclosed to out-of-state officials investigating sexual health related matters. Technology companies should be required to change their internal policies and procedures to ensure that they collect and disclose minimal information from consumers and adopt notification procedures for when data could be sold, giving people a chance to fight back against surveillance aimed at their personal health information.

Of the bills before you today, only LD 1822 contains provisions that would end the needless collection of sensitive information like location and biometric data and outlaw the use of search word and geofencing warrants, which allow police to conduct dragnet-like surveillance.[11]

The recent rollbacks of the right to privacy should serve as a reminder to us all that we should never accept living in a surveillance society, no matter what technology is used to carry it out. The right to privacy sits at the heart of democracy, and we must fight to ensure its relevance now and in the decades to come.

To facilitate strong consumer privacy protections, please vote ought to pass on LD 1822 and ought not to pass on LDs 1088, 1224, and 1284.

---

[9] Biometric Information Privacy Act, 740 ILCS 14/1 et seq. (2008).
[10] Ashton Harris et al., *Analyzing Virginia's New PRA for Protecting Consumer Reproductive and Sexual Health Information*, ByteBack, Apr. 24, 2025, available at https://www.bytebacklaw.com/2025/04/analyzing-virginias-new-pra-for-protecting-consumer-reproductive-and-sexual-health-information/.
[11] LD 1088 also contains an anti-geofencing provision, but its data minimization provision would allow any collection or use of data as long as it is disclosed in a privacy policy. *See* LD 1088, p. 10, lines 7-20.