epic.org | Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 22, 2023

The Honorable Anne Carney, Senate Chair
The Honorable Matt Moonen, House Chair
Maine State Legislature
Judiciary Committee
230 State Street
Augusta, Maine 04330

Dear Chair Carney, Chair Moonen, and Members of the Committee:

EPIC writes in support of LD 1902 regarding the privacy of personal health data. Health data is among the most sensitive forms of personal data, yet there are few settled rules regarding the sharing and use of this data.[1] LD 1902 gives the Maine Legislature the opportunity to prevent the mass collection and monetization of Mainers' sensitive health data. A similar law was recently enacted in Washington State.[2]

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[3] This testimony is based largely on an analysis done by EPIC Fellows Sara Geoghegan and Dana Khabbaz in 2022.[4]

Current Law Fails to Adequately Protect Health Data

Since the creation of the Hippocratic Oath around 400 B.C., protecting the privacy of patients has been a key component of the physicians' code of conduct. However, over time, health information use has expanded into many organizations and individuals who are not subject to medical ethics codes, including employers, insurers, government program administrators, attorneys, and others. Additionally, advancements in technology have given rise to fitness trackers, wearable devices, extended reality technology, and other new gadgets that collect, process, and make inferences relating to health information. Many assume that the Health Insurance Portability and Accountability Act (HIPAA) protects their health information generally, when in fact most of the health data collected outside of the doctor/patient or insurance relationship is not covered by HIPAA.[5]

---

[1] EPIC, *Full of Holes: Federal Law Leaves Americans' Personal Data Exposed* (Apr. 27, 2023), https://epic.org/full-of-holes-federal-law-leaves-americans-personal-data-exposed/.
[2] EPIC, *Washington State Legislature Passes Health Data Privacy Law* (Apr. 18, 2023), https://epic.org/washington-state-legislature-passes-health-data-privacy-law/.
[3] EPIC, *About EPIC*, https://epic.org/about/.
[4] Sara Geoghegan and Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism* (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/.
[5] Sara Morrison, *HIPAA, the health privacy law that's more limited than you think, explained*, Vox (Jul. 30, 2021)

The recent Supreme Court decision in *Dobbs v. Jackson Women's Health Organization* poses an unquestionable threat to the safety and privacy of abortion providers and patients. The implications are all the more harrowing in light of the technological realities of today: a huge data broker industry that sells our location data and most sensitive information to private and government purchasers alike.

We are only beginning to witness the impact of the *Dobbs* decision on individual privacy.[6] The decision poses a critical threat to privacy rights when combined with today's vast personal data collection systems. If a woman travels to Maine from a state where abortion is illegal in order to obtain reproductive care, law enforcement in her home state could obtain the data collected about her location, her online activity, and more either by purchasing it from a data broker or via subpoena. LD 1902, by limiting the amount of health data collected on individuals, will limit law enforcement's ability to prosecute a woman for obtaining a legal abortion in Maine.

Mass Collection of Location Data Is Particularly Harmful to Those Seeking Health Care

Commercial and government entities collect vast amounts of personal information about individuals, including location data. Location data can reveal the most sensitive characteristics about a person, including their health conditions or status. Phones and devices generate location data which is collected by various entities and may be sold to data brokers, advertisers, or the government.

Data brokers use secret algorithms to build profiles on every consumer based on their online activities, often without the consumer's knowledge. Using profiles to target advertisements to pregnant people is not new. In 2012, it was reported that Target sent maternity and pregnancy related advertisements to a teenager before she told her family she was pregnant.[7] As the article, *Target Knows You're Pregnant*, explained:

> All Target customers are assigned a Guest ID. Associated with this ID is information on 'your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit.'

Analyzing this data, combined with a customer's purchase history, could produce a "pregnancy prediction" score, which includes an estimate of the customer's due date. Post *Roe*, these types of profiles (which have become even more invasive and sophisticated in the past decade) could be weaponized against individuals who seek abortions in states where abortion is illegal. LD 1902 would help prevent this type of targeting by placing limits on the collection of health data and prohibiting the sale of such data.

Data brokers play a pervasive role in the location data market. Data brokers buy, aggregate, disclose, and sell billions of data points on Americans, including their location data. They operate with effectively no oversight or regulation. Data brokers collect health information, including period

---

[6] Cat Zakrzewski, et al., *Texts, web searches about abortion have been used to prosecute women*, Wash. Post (July 2022), https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/.
[7] Kelly Bourdet, Target Knows You're Pregnant (Feb. 2012), https://www.vice.com/en/article/qkkepv/target-knows-you-re-pregnant.

tracking information.[8] Brokers also collect information from the sites individuals visit online and the advertisements that they click on, and make inferences from this data. And, thanks to the proliferation of smartphones and wearables, data brokers collect and sell real-time location data.[9]

Advertising companies also collect and use location data, including the location of sensitive location such as abortion clinics, as well, and advertisers can use that information to target people. Just last week, the Wall Street Journal reported that an antiabortion group was using phone location data to target advertisements to individuals who visited Planned Parenthood clinics.[10] The article reported:

> The aim of the campaign was to educate women about alternatives to terminating a pregnancy, according to a Veritas Society website that was online until late last year. On that site, Veritas Society said it could identify phones on the premises of abortion clinics and extract their device IDs—the unique identifiers given by Apple and Google to mobile devices to help advertisers target consumers across phone apps and websites. With such IDs and some basic analysis, it is sometimes possible to link a phone to a real-world address, and potentially a name, the Journal has previously reported. It couldn't be learned whether Veritas Society took that step. "We captured the cell phone IDs of women who visited all Planned Parenthood locations in Wisconsin along with similar locations and their associated parking areas," the Veritas Society website said.

This practice, where an entity defines a geographical boundary and targets mobile devices within that boundary, is known as geofencing. LD 1902 would prohibit this form of geofencing around an entity that provides in-person health care services. This is a critical measure that would protect Mainers from this extremely invasive targeting and manipulation.

Suggested Amendment: Remove Consent Option

EPIC would recommend a change to LD 1902 to remove the option for entities to collect consumer health data with consent even if the collection of such data is not strictly necessary to provide the service the individual has requested. The best protection would be to restructure §1350-Q so that regulated entities may only collect consumer health data if "strictly necessary" to provide a product or service that the consumer has requested. This change was made to similar bill in Congress when it was reintroduced earlier this month.[11] It is also the requirement for the collection of sensitive

---

[8] Justin Sherman, *Your Health Data Might Be for Sale*, Slate Future Tense (June 2022), https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

[9] Jon Keegan and Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

[10] Byron Tau and Patience Haggin, Antiabortion Group Used Cellphone Data to Target Ads to Planned Parenthood Visitors, Wall Street Journal (May 18, 2023), https://www.wsj.com/articles/antiabortion-group-used-cellphone-data-to-target-ads-to-planned-parenthood-visitors-446c1212?st=1581hk7jp9lm35x&reflink=desktopwebshare_permalink.

[11] Congresswoman Sara Jacobs, *Rep. Sara Jacobs Leads Reintroduction Of My Body, My Data Act To Protect Reproductive And Sexual Health Data* (May 17, 2023), https://sarajacobs.house.gov/news/documentsingle.aspx?DocumentID=786.

data in the American Data Privacy and Protection Act in Congress, which was favorably reported by the House Energy & Commerce Committee on a 53-2 bipartisan vote last session and is expected to be reintroduced soon. This standard would prevent consent fatigue by consumers by placing a baseline limit on when entities may even ask to collect sensitive health data.

Conclusion

Health data has long been considered sensitive. It is time for our laws to catch up to technology. The obligation to protect and limit the collection of health data should fall on the entities collecting it, not individuals seeking health care. We urge the Committee vote "ought to pass" on LD 1902.

If EPIC can be of any assistance to the Committee, please contact EPIC Deputy Director Caitriona Fitzgerald at fitzgerald@epic.org.

Sincerely,

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Deputy Director