AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

ACLU OF RI POSITION: SUPPORT

TESTIMONY ON 25-H 5857,
RELATING TO HEALTH AND SAFETY – REPRODUCTIVE FREEDOM AND GENDER AFFIRMING CARE HEALTH DATA PRIVACY ACT
April 23, 2025

The ACLU of Rhode Island strongly supports this legislation and its critical safeguards for the privacy of reproductive and gender-affirming healthcare data.

The vast amount of personal data collected daily by companies, sometimes without our consent or knowledge, underscores the need for the protective measures outlined in this legislation. Specifically, this bill would require entities to obtain explicit consent from individuals before collecting or sharing any data related to that individual's reproductive or gender-affirming care. Also under this bill, consent to sell this data must meet specific and heightened requirements. Additionally, any data collected must be restricted to what is necessary to provide the services requested by the user.

The bill's coverage is directed at those entities that are not covered by HIPAA but provide reproductive and gender-affirming healthcare services, collect reproductive and gender-affirming healthcare data from individuals in providing those services, and direct the collection and use of the data. These include services or products provided by many modern health apps, including those that track health conditions, like period-tracking apps or apps that monitor vital statistics, to the extent they relate to reproductive and gender-affirming care. However, only information that can directly identify a person's reproductive or gender-affirming health status is covered by the bill.

This bill would also prohibit entities from creating a geofence around healthcare facilities that provide reproductive or gender-affirming services in order to track individuals seeking care. A geofence is a virtual boundary drawn around certain areas that tracks when a user has entered or left the boundary area. For example, a map application that has access to your location for navigation purposes cannot use that data to secretly identify healthcare clinics someone has visited.

Last session, the General Assembly passed the Healthcare Provider Shield Act. This act created broad protections for Rhode Island health care providers from out-of-state legal action, specifically from places where abortion and other reproductive or gender-affirming care has been limited because of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*. Protecting data that could indicate reproductive or gender-affirming status is the next logical step in protecting reproductive rights and reaffirming our commitment to being a safe harbor for our residents and those who seek this necessary care here in Rhode Island.

We would note that a proposed Sub A of this legislation has been crafted after consultation with various stakeholders. The Sub A makes clarifying changes to the bill, and we support those proposed amendments which do not change the core of the legislation in any way.

Some examples of the need for this bill are contained in the two attached documents that our National ACLU office has prepared in support of this critical information. Cell phone tracking and data collection represent both a powerful tool and a comprehensive surveillance scheme. Passage of this legislation will preserve the legitimate use of this technology and the individual privacy rights of all Rhode Islanders. For these reasons, we urge passage of this bill.

Rhode Island Reproductive Health and Gender-Affirming Healthcare Data Privacy Act

H5857 / S824

CRITICAL GAPS IN PROTECTING REPRODUCTIVE AND GENDER-AFFIRMING HEALTHCARE MUST BE FILLED

Health-related data held by fitness apps, period trackers, and retailers may not be subject to the federal Health Insurance Portability and Accountability Act, which is limited to traditional healthcare providers and related entities. These unregulated apps and companies share health data with third parties for various purposes, often without our explicit consent. For example:

- An **analysis** of the 15 biggest fitness apps revealed that 80% of them track and share our health data with third parties. Fitness apps are particularly vulnerable to data breaches. In 2021, an unsecured database containing over 60 million records from wearable technology and fitness services — including Apple's HealthKit and Fitbit — was **exposed**. The data released included names, dates of birth, weight, GPS logs, and gender.
- Period-tracking apps raise particularly high risks for misuse of health data. The apps **MIA Fem and Maya** have been found to share data such as the use of contraception and menstrual cycles with third parties — such as Facebook — often without telling their users. **Flo Health**, the developer of a widely used fertility-tracking app, settled with the FTC in 2021 over allegations that they shared users' menstrual cycles, ovulation dates, pregnancy plans, and symptoms with Facebook and Google despite promising to keep such information private.
- Retailers, such as Amazon and Walgreens, have deeper insight into our health than many may realize. **Amazon** has been able to infer our medical conditions based on our shopping history and is using the health data they collect on us to recommend prescriptions and treatments. **Walgreens** was sued in 2011 for selling prescription information to third parties.

Concerns about abuse of our health data have become even more pronounced as other states have increased their prosecution of protected healthcare in Rhode Island — reproductive and gender-affirming care. The Rhode Island Reproductive Health and Gender-Affirming Healthcare Data Privacy Act would provide crucial protection for reproductive and gender-affirming healthcare data.

THE BILL WOULD PROVIDE CRUCIAL SAFEGUARDS

Entities regulated by the bill would be required to meet common-sense protections for data related to our reproductive and gender-affirming healthcare:

- To collect and use our information, entities would have to obtain clear, affirmative opt-in consent. No more shady practices buried in lengthy, confusing privacy policies.
- Our reproductive and gender-affirming healthcare data could only be limited to a few purposes such as: providing the services we request, fulfilling our orders, complying with legal obligations, protecting public health and safety, preventing fraud, responding to cybersecurity attacks, and investigating illegal activity.
- Consent to sell our reproductive and gender-affirming healthcare data must meet specific, heightened requirements.

- Entities covered by the bill would have to implement cybersecurity protections and ensure their contractors protect our reproductive and gender-affirming healthcare data.

THE BILL IS FOCUSED AT THE POINT OF COLLECTION

The bill's coverage is targeted at the entities that have raised the greatest concerns with increased attacks on reproductive and gender-affirming healthcare: those that **do all three of the following:** (1) provide reproductive and gender-affirming healthcare services; (2) collect reproductive and gender-affirming healthcare data from individuals in providing those services; **and**, (3) direct the collection and use of the data. Thes are called "**regulated entities**."

Reproductive and gender-affirming healthcare services extend beyond traditional healthcare and include the services or products provided by many modern health apps: tracking our health conditions and statuses, logging purchases of medications, and monitoring our vital statistics, to the extent they are related to reproductive and gender-affirming healthcare.

COVERAGE FOR LOCATION DATA AND ONLINE ACTIVITY

Our location data and online activity reveal the most sensitive aspects of our lives — including where we receive healthcare or our efforts to research our care. For example:

- The FTC has brought actions against **data brokers** for selling the location data of people who visit medical facilities, domestic abuse shelters, and places of worship.
- Location data obtained from **Strava** — a health and fitness app — has exposed sensitive military base locations because the app shares users' fitness data publicly by default. That health and location data can then make its way to **data brokers**, where it is readily available to anyone — even foreign adversaries.
- Several entities, including hospitals, health websites, and **pharmaceutical companies**, are using our health data to bombard us with targeted advertising. Emergency room patients have reported **seeing ads** for personal injury attorneys based on their location. We should not have to deal with solicitations while trying to receive treatment for our illnesses.
- **Google** and **Facebook** have worked with pharmaceutical companies and health clinics to target social media users with ads for treatment options based on data the companies gather about their users. Amazon, which now has a pharmacy line of business, is using your data to infer your health history and **target you with ads for prescription drugs**.

Consequently, the bill covers regulated entities' collection and use of both (1) "precise location information that could reasonably indicate a consumer's attempt to acquire or receive" reproductive and gender-affirming healthcare and (2) individuals' "efforts to research or obtain gender-affirming care-related services."

Finally, all entities — even those not regulated by the bill's other provisions — would prohibited from using a geofence around reproductive and gender-affirming healthcare facilities to identify individuals receiving reproductive and gender-affirming healthcare.

Examples of Health Data Harms

NOT ALL HEALTH DATA IS HIPAA-PROTECTED, AND NOW IT'S FOR SALE

Health-related data held by fitness apps, period trackers, retailers, and employers may not be subject to HIPAA, which is limited to traditional healthcare providers and related entities. These unregulated apps and companies share health data with third parties for various purposes, often without our explicit consent. For example:

- An analysis of the 15 biggest fitness apps revealed that 80% of them track and share our health data with third parties. Fitness apps are particularly vulnerable to data breaches. In 2021, an unsecured database containing over 60 million records from wearable technology and fitness services — including Apple's HealthKit and Fitbit — was exposed. The data released included names, dates of birth, weight, GPS logs, and gender.
- Period-tracking apps raise particularly high risks for misuse of health data. The apps MIA Fem and Maya have been found to share data such as the use of contraception and menstrual cycles with third parties — such as Facebook — often without telling their users. Flo Health, the developer of a widely used fertility-tracking app, settled with the FTC in 2021 over allegations that they shared users' menstrual cycles, ovulation dates, pregnancy plans, and symptoms with Facebook and Google despite promising to keep such information private.
- Retailers, such as Amazon and Walgreens, have deeper insight into our health than many may realize. Amazon has been able to infer our medical conditions based on our shopping history and is using the health data they collect on us to recommend prescriptions and treatments. Walgreens was sued in 2011 for selling prescription information to third parties.
- Employers, such as Activision Blizzard and Yale University, have accessed health-related data through mandatory wellness programs to make employment decisions. Activision used data from a pregnancy-tracking app to determine return to work timelines, and Yale fined employees if they refused to undergo medical tests under their employee wellness program.
- Several mental health and addiction treatment apps and services, including Betterhelp, Cerebral, and Monument Inc, have shared user data with third parties – including social media companies. A 2019 study of the 36 largest mental health apps found that 92% of them have shared user data with advertisers.

EXPLOITING OUR LOCATION DATA IS A HEALTH AND NATIONAL SECURITY ISSUE

Our location data reveal a multitude of the most sensitive aspects of our lives — where we receive healthcare, work, live, worship, and protest. It can go so far as to revealing sensitive national security information, including the locations of US military bases:

- The ability for data brokers to track our location data is an intrusion on our personal lives and health privacy. The FTC has brought actions against **data brokers** for selling the location data of people who visit medical facilities, domestic abuse shelters, and places of worship.
- The practice of tracking and selling location data is so invasive that it can be used to "track Americans in and around churches, **military bases**, and doctors' offices." Location data obtained from **Strava** — a health and fitness app — has exposed sensitive military base locations because the app shares users' fitness data publicly by default. That health and location data can then make its way to data brokers, where it is readily available to anyone — even foreign adversaries.

USING OUR HEALTH DATA FOR TARGETED ADVERTISING

When we entrust our health data to anyone, the last thing we want is for that data to end up in a stranger's hands. Even more intrusive is the use of that data to target us for ads.

- Several entities, including hospitals, health websites, and **pharmaceutical companies**, are using our health data to bombard us with targeted advertising. Emergency room patients have reported **seeing ads** for personal injury attorneys based on their location. We should not have to deal with solicitations while trying to receive treatment for our illnesses.
- **Google** and **Facebook** have worked with pharmaceutical companies and health clinics to target social media users with ads for treatment options based on data the companies gather about their users. Amazon, which now has a pharmacy line of business, is using your data to infer your health history and **target you with ads for prescription drugs**.

PRICE DISCRIMINATION AND RISK PROFILING

Health and life insurance companies are able to gather our health data without our knowledge and use that information to determine our premiums and coverage.

- **Bill**, a healthy 60-year-old interviewed by The Atlantic in November 2024, was denied long-term care insurance after he discovered he had a genetic mutation linked to ALS — despite the fact that he did not have ALS.
- **Kelly Kashmer** (42) from South Carolina was denied life insurance after receiving results indicating a high-risk BRCA2 genetic mutation.
- A 2018 **NPR article** highlighted concerns that while federal law prohibits health insurers from using genetic information, life insurers can still use such data to influence coverage decisions.
- **United Health** deployed a faulty AI system to analyze personal information to deny patients medically necessary coverage.

THE WEAPONIZATION OF OUR HEALTH DATA

We should never feel uncomfortable seeking medical care, but with our health data for sale, promises made are not promises kept. Health data has been weaponized against certain individuals in furtherance of certain political and social agendas.

- Health data obtained from **cell phone records**, private conversations on social media, and **internet search results** have been used to prosecute several individuals who have attempted to receive medical care.
- **State law enforcement** have misused Medicaid authority to obtain private medical records from healthcare providers offering care to transgender individuals and have weaponized that data against transgender youth and adults.