ACLU of Massachusetts
One Center Plaza, Suite 850
Boston, MA 02110
617-482-3170
www.aclum.org

June 26, 2023

Joint Committee on Consumer Protection and Professional Licensure
Sen. John J. Cronin and Rep. Tackey Chan, Co-Chairs

Testimony in Support of H.357 and S.148

An Act Protecting Reproductive Health Access, LGBTQ lives, Religious Liberty, and Freedom of Movement by Banning the Sale of Cell Phone Location Information

Dear Senator Cronin, Representative Chan, and members of the committee,

The ACLU of Massachusetts offers our strongest support for H.357 and S.148, the *Location Shield Act*, sponsored by Representatives Kate Lipper-Garabedian and Senator Cynthia S. Creem.

Location information collected from our personal devices enables companies to provide us with services that make our lives easier. Yet location data is also among the most sensitive types of information, prone to abuse and misuse that can have dramatic consequences for individuals and families.[1] Today, no law prevents companies like the makers of smartphone applications from selling this personal information, and so it is openly stockpiled and sold, allowing purchasers to track our movements and activities wherever we go, exposing all of us to the threat of grave harm.

The legislation before you proposes a simple and straightforward solution to this problem by prohibiting the sale and monetization of personal location information derived from devices physically present in the state of Massachusetts. According to a poll conducted by Beacon Research, 92 percent of Massachusetts likely voters support this reform. Enacting these popular location privacy protections will make Massachusetts a leader in protecting reproductive health access, LGBTQ+ lives, religious liberty, and freedom of movement for all, setting a precedent for the rest of the nation and the world to follow.

June 24, 2023 marked the one-year anniversary of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, which overturned *Roe v. Wade* and significantly increased the urgency of this legislation. What before *Dobbs* would have been "merely" a vitally important consumer privacy protection measure is now imperative. The purpose of this bill is to protect the location privacy of all cellphone users. As such, it knows no ideology. Nonetheless, in the wake of *Dobbs* its provisions will be particularly impactful for people seeking health care, such as abortion or gender affirming care, that is lawfully protected in Massachusetts and prohibited and singled out for hostility in other parts of the country.

What is Location Information?

Location information is the subset of personal information that **reveals the specific geographical position of a particular device, such as a cell phone or wearable technology, and therefore**

1 Jennifer Valentino-Devries et al., Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, The New York Times, December 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

the person carrying or wearing it. Almost all adults, and many children, carry cell phones with them everywhere they go, and millions wear electronic health trackers. These widely-used consumer technologies create billions of data points revealing the locations of their users—every day, everywhere, at nearly every moment.[2]

Consumers enjoy many conveniences when their devices can quickly map their locations to provide, for example, weather updates, nearby amenities, and driving directions. The Location Shield Act therefore does not prohibit companies from collecting location information or using it to provide people with requested services. **But most people are unaware that many apps are not merely using their location data to provide them with a service—they are turning around and selling it to third parties.** It is this transfer of our most sensitive personal information to third parties that the Location Shield Act aims to stop.

The Federal Government Has Recognized Location Data is Extremely Sensitive, But No Law Protects Consumers

In 2020, the Federal Communications Commission (FCC) took action against telecommunications providers for selling customer cellphone location information. The FCC notified telecoms that section 222 of the Communications Act of 1934 prohibits them from selling customer location information, because that information is customer proprietary network information, which is subject to strict regulation and privacy protection. The FCC correctly identified cellphone location information as "highly personal and sensitive," and has taken aggressive action to punish telecoms who violate the law and sell customer location data.[3]

But while the FCC has used its authority under the Communications Act to prevent *telecommunication companies* like T-Mobile and Verizon from selling customer cellphone location data, it has *no such authority* to forbid the practice in other industries, including the companies that produce the applications that make our cellphones "smart." As a result, the very same kind of information the FCC took action to protect from telecom disclosure is available for sale on the open market—as long as it comes from another source, such as smartphone apps.

In recent years, the United States Supreme Court and the Federal Trade Commission (FTC) have likewise recognized the extreme sensitivity of cellphone location information.

In a 2018 ruling in *Carpenter v. United States*, the high court held that police must obtain a warrant to access stored cellphone location information, because it "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[4]

Most recently, in 2022, the FTC filed suit against location data broker Kochava, arguing that selling the personal cellphone location data of millions of unsuspecting people constitutes an unfair business practice.[5] The FTC alleged that Kochava "purchased vast troves of location information

---

2 Companies employ numerous methods to monitor consumers and gather their location information, including global positioning systems ("GPS"), software development kits ("SDK"), real-time bidding ("RTB"), Bluetooth, Wi-Fi, and cell site location information ("CSLI"). Together, the data paints a full picture of a person's movements, activities, and life. See Bennet Cyphers, Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It, EFF, March 19, 2020. https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and

3 See NOTICE OF APPARENT LIABILITY FOR FORFEITURE AND ADMONISHMENT, FCC, ps. 41-49, https://docs.fcc.gov/public/attachments/FCC-20-27A1_Rcd.pdf.

4 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)

5 FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations, August 29, 2022, FTC.gov. https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

derived from hundreds of millions of mobile devices," including those of people traveling to and from sensitive locations like "reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities."[6] Unfortunately, in May 2023 a federal court in Idaho granted the data broker's motion to dismiss the lawsuit,[7] but the FTC remains deeply concerned and has refiled the case.

The takeaway from these varied actions is simple. **Multiple branches of the federal government are delivering a consistent message: location data is extremely sensitive and requires robust protection.** Nonetheless—even though the FCC has banned telecoms from selling cellphone location data, the Supreme Court has required police to get a warrant before demanding cellphone location data from telecoms, and the FTC has alleged that the sale of cellphone location data constitutes an unfair practice violating the privacy of hundreds of millions of Americans—**no existing law prohibits non-telecom companies from selling these records on the open market.** As a result, it remains the case that a vast and varied market allows anyone with sufficient funds to buy cellphone location information revealing the most sensitive personal aspects of millions of people's lives.[8]

The Sale of Location Data Directly and Gravely Harms Consumers

The location information market allows companies, individuals, and government actors to obtain detailed, comprehensive personal information about millions of people. Information is power, and purchasers of this powerful information can use it to infer extremely sensitive facts about people's private lives and associations. Then they can weaponize that information to harm people, families, and communities.[9]

Unlike many other types of data, it is functionally impossible to anonymize location information when it is amassed in large quantities. Location information at scale is inherently identifiable. Where a phone is every night reveals where a person lives, and where that phone goes during the day reveals where the person works or goes to school, making it trivial to connect a supposedly "anonymous" device to a real human being.

As the FTC has recently asserted, the sale of location information exposes individuals "to stigma, discrimination, physical violence, emotional distress, and other harms."[10] These harms are particularly acute for people experiencing or trying to disengage from abusive relationships, those targeted by stalkers, and people subjected to threats and harassment because of their political or social views, or their race, religion, sexuality, or gender. The existence of the location data market also undermines existing state laws that aim to keep the personal information of law enforcement officers confidential as a means to protect their personal safety and that of their family members.

This harm is real. In at least two cases, right-wing organizations have used location information for expressly political purposes. In one case, a billionaire-funded project purchased location information

---

6 Ibid.

7 "Judge Dismisses F.T.C. Lawsuit Against a Location Data Broker," Natasha Singer, New York Times, May 5, 2023. https://www.nytimes.com/2023/05/05/business/ftc-kochava-location-data.html

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

9 Joseph Cox, The Inevitable Weaponization of App Data Is Here, Vice, July 20, 2021. https://www.vice.com/en/article/pkbxp8/grindr-location-data-priest-weaponization-app

10 FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations, Federal Trade Commission, August 29, 2022. https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

and used it to out priests suspected of engaging in same sex relationships.[11] At least one priest was publicly named, humiliated, and fired;[12] according to news reports, others' careers were quietly derailed. In another case, a right-wing think tank used location information to demonstrate how migrants who enter the United States through the U.S.-Mexico border travel and settle throughout the country, turning the data into a political weapon wielded to incite anti-immigrant attitudes and policies.[13]

Location Data Endangers Patients in the Post-Dobbs Era

It is only a matter of time before anti-abortion extremists use commercially available location data to go after abortion providers and their patients. And the prospect of what they might do when they can track people's movements using this personal information is chilling.

In post-*Dobbs* America, abortion hostile state governments and individual civil litigators[14] are seeking to control and—and flatly deny—reproductive autonomy through the application of criminal and civil laws.[15] **The widespread availability of detailed and personally identifiable location information allows out-of-state law enforcement agencies and bounty hunters to conduct broad fishing expeditions, looking for targets for harassment and worse**.

Police across the country lawfully access digital data in criminal investigations by serving legal demands on companies.[16] But while police need individualized suspicion and a warrant to access location data via these traditional means, the availability of location information in a commercial marketplace allows police in abortion hostile states to conduct fishing expeditions *looking for targets*. Bounty hunters eager to initiate civil litigation under a law like Texas' SB8 could likewise buy location information showing them who has traveled from an abortion hostile state to a Planned Parenthood clinic in Massachusetts.[17]

And the data is right there waiting for them. After the leak of the *Dobbs* decision, a reporter found that data brokers were selling location information of people who visited abortion clinics.[18] In its investigation of data broker Kochava, the FTC examined data collected from more than 61 million mobile devices and found "the data could be used to identify people who have visited a reproductive health clinic." The FTC found that this data sample allowed a buyer "to track a mobile device from a reproductive health clinic to a single-family residence to other places routinely visited," enabling

11 "Catholic group spent millions on app data that tracked gay priests," Michelle Boorstein and Heather Kelly, Washington Post, March 9, 2023. https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/

12 "Priest outed via Grindr app highlights rampant data tracking," the Associated Press, July 22, 2021. https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493

13 "Oversight Project Investigation Uncovers Shocking Facts About Who's Facilitating Biden Border Crisis," Heritage Foundation, December 5, 2022. https://www.heritage.org/press/oversight-project-investigation-uncovers-shocking-facts-about-whos-facilitating-biden-border

14 Erin Coulehan, Abortion "Bounty" Laws in States Like Texas and Oklahoma: How They Work, Teen Vogue, July 7, 2022. https://www.teenvogue.com/story/abortion-bounty-laws

15 After Roe Fell, Center for Reproductive Rights. https://reproductiverights.org/maps/abortion-laws-by-state/

16 Runa Sandvik, How US police use digital data to prosecute abortions, TechCrunch, January 27, 2023. https://techcrunch.com/2023/01/27/digital-data-roe-wade-reproductive-privacy/

17 Jon Keegan, Planned Parenthood Data Found on Another Location Data Dashboard, The Markup, July 15, 2022. https://themarkup.org/privacy/2022/07/15/planned-parenthood-data-found-on-another-location-data-dashboard

18 Joseph Cox, Data Broker Is Selling Location Data of People Who Visit Abortion Clinics, May 3, 2022, https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood

the identification of not only patients but "medical professionals who perform, or assist in the performance, of reproductive health services."[19]

As a leader on reproductive freedom, Massachusetts must take the cellphone location data of people traveling within the Commonwealth off the market before it is abused by anti-abortion extremists.

The Location Data Market Harms Society and Individual Rights

In addition to the threats that the location data market poses to individuals as they attempt to exercise their right to access health care or go about their lives free from targeted harassment or discrimination, it also endangers fundamental aspects of civil society in myriad ways. Location data sales jeopardize and chill the exercise of constitutional rights, especially First Amendment rights.[20] Algorithms and automated decision systems can leverage commercially available location information in ways that lead to systemic discrimination.[21] The availability of location information in an open, unregulated market allows foreign governments, organized criminals, political extremists, and counter-intelligence agencies to track American researchers, intelligence agents, and military and law enforcement officials.[22] And, finally, this market can provide the means for the government to buy location information and circumvent the traditional protections of the Fourth Amendment to the U.S. Constitution.[23]

As the FTC, Supreme Court, and FCC have recognized, **our personal location information reveals the most sensitive and intimate details about each of us.** We all deserve to live in a society that imposes clear and enforceable laws to keep that information private.

Massachusetts Voters Believe the Legislature Must Act to Protect Location Privacy

According to a Beacon Research poll commissioned by the ACLU, more than 9 in 10 Massachusetts likely voters support legislation to ban the sale of cellphone location information. Voters know how sensitive these records are, and they do not think it is acceptable that companies today can freely sell and trade this information.[24]

---

19 Complaint for Permanent Injunction and Other Relief, F.T.C. v. Kochava Inc., Case No. 2:22-cv-377, U.S Dist. Court for the District of Idaho. https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf

20 Joseph Cox, How the U.S. Military Buys Location Data from Ordinary Apps, Vice, November 2020.

https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

21 Ketan Doshi, Leveraging Geolocation Data for Machine Learning: Essential Techniques, Towards Data Science, April 17, 2021. https://towardsdatascience.com/leveraging-geolocation-data-for-machine-learning-essential-techniques-192ce3a969bc; Center for Strategic & International Studies, Disability Discrimination and Automated Surveillance Technologies, Transcript, August 25, 2022. https://www.csis.org/analysis/disability-discrimination-and-automated-surveillance-technologies

22 Last year, U.S. Senators slammed Google after the company allegedly shared information, including location information, with a Russian ad-tech company owned by Russia's state bank. This data sharing occurred even after the United States Treasury in February 2022 placed the Russian firm on a sanctions list. Craig Silverman, Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months, ProPublica, July 1, 2022. https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine#1364281

23 In Carpenter, Chief Justice Roberts held that these records deserve constitutional protection because mapping a cellphone's location "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations." Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2206; 201 L. Ed. 2d 507. See also Bennett Cyphers, How the Federal Government Buys Our Cell Phone Location Data, EFF, June 13, 2022. https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data

24 Voters were asked, "Massachusetts is considering a new law prohibiting the sale of location data. Would you support or oppose passing a state law to prohibit companies from selling your location data?" 92 percent of respondents said they would support such a law. ACLU of Massachusetts and Beacon Research, Statewide Voter Support Poll Overview, Your Location Is Not Their Business, June 14, 2023. https://www.aclum.org/sites/default/files/field_documents/your_location_its_none_of_their_business_-_public_deck.pdf

Massachusetts can protect people by banning the sale of cell phone location information and lead the nation by passing this popular, vitally important privacy reform. Indeed, the Beacon Research poll found that by a 3-to-1 margin, voters think the state has a responsibility to do so.

Massachusetts voters are correct. The Commonwealth cannot leave this issue to industry self-regulation or individual cellphone users to attempt to manage by themselves through opt-out measures. The opt-out myth is particularly pernicious, because consumers' understanding of their options and what is on the line for their privacy is vastly outmatched by companies' ability to manipulate and obscure; consumers would need to individually opt out of the sale of their location data for every single app; and companies could make such an opt-out only available to consumers pay for premium services, making privacy a luxury and discriminating against low-income consumers. Furthermore, enforcing a location privacy law that relies on an opt-out framework would be close to impossible. The only way to ensure location information is not abused is to prohibit its sale.[25]

The Location Shield Act

The Location Shield Act provides robust location privacy protection for people using cellphones and wearable devices in the state of Massachusetts.

The heart of the bill bans companies from selling, renting, trading, or leasing location information to third parties. The intended impact of this legislation is to ensure no data from devices physically present in Massachusetts ever appears in data broker databases.[26]

In addition, the legislation establishes several substantive protections regarding the disclosure of location information. It prohibits companies from disclosing an individual's location information to third parties except for defined reasons: if such disclosure is necessary to carry out the permissible purpose for which they collected the information in the first place; if such disclosure is requested by the individual; or if the disclosure is required by another law.

Importantly, the Location Shield Act in no way interferes with law enforcement's established ability to access location data to conduct investigations with judicial authorization or respond to public safety crises. The legislation allows companies to share location data with law enforcement as they do today, in response to a warrant or an emergency.

Finally, the legislation sets basic standards for how companies collect location data and for what purpose. It requires companies to obtain consent before collecting location data and allows technology users to opt-out of location-based advertisements, if they so choose. It also includes data minimization provisions to ensure that companies do not collect more location data than necessary, delete the data after it is no longer needed, and only use the data for authorized purposes.

---

25 Another approach is to require companies to obtain affirmative opt-in consent before selling location data. The Illinois Biometric Information Privacy Act employs this opt-in framework, backed by a strong private right of action. A properly constructed opt-in framework of this kind may be able to provide meaningful privacy protection.

26 It is worth noting, for purposes of constitutional analysis, that this ban is evenhanded. It does not discriminate based on the seller or based on their motives. It prohibits both government and private parties from selling location data. Prohibiting the sale of data by a particular class of speakers or distinguishing between commercial and non-commercial uses of data in a discriminatory manner can raise constitutional concerns about restrictions on speech. This proposal avoids those issues because (i) it does not impose a speaker-based burden and (ii) it does not hinge on whether the data is used for commercial or non-commercial purposes.

Likewise, the bill complies with the Commerce Clause in the U.S. Constitution. First, it does not discriminate against out-of-state actors; its provisions apply equally to companies inside Massachusetts and those outside of the Commonwealth. Second, the Commonwealth's substantial interest in protecting the privacy and safety of its residents outweighs any limited burden on interstate commerce. In this respect, the proposed legislation operates like many other state consumer protection and data privacy laws.

Like all meaningful consumer protection and civil rights laws, the Location Shield Act also includes enforcement mechanisms, without which it would be ineffective. The legislation enables claims on behalf of the public by the state Attorney General, as well as claims by individuals whose location data is misused in violation of the law. A robust private right of action is necessary in order to ensure the legislation achieves its goal of protecting location privacy.

Conclusion

Massachusetts has an historic opportunity to continue to legislate in favor of basic human and civil rights. The Location Shield Act will, if enacted, protect all people in the Commonwealth from the grave harms that flow from the sale of their most personal and sensitive information.

We respectfully urge the Committee to advance this crucial legislation with a favorable report. Thank you.