# The Location Data Market, Data Brokers, and Threats to Americans' Freedoms, Privacy, and Safety

Written Testimony

Justin Sherman
Senior Fellow and Research Lead, Data Brokerage Project
Duke University Sanford School of Public Policy

Massachusetts Legislature

Joint Committee on Consumer Protection and Professional Licensure

Hearing on Pending Legislation

June 26, 2023

---

Distinguished members of the Committee, I appreciate the opportunity to testify about location data and threats to Americans' freedoms, privacy, and safety.

I am a senior fellow at Duke University's Sanford School of Public Policy, where I lead our research project on the data brokerage ecosystem. We study the virtually unregulated industry and practice of data brokerage—the collection, inference, aggregation, analysis, buying, selling, and sharing of data on individuals—and its impacts on civil rights, consumer privacy, personal safety, and national security. I am also the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm, and a nonresident fellow at the Atlantic Council, where I work on cybersecurity, privacy, internet policy, and geopolitical issues.

The market for location data threatens Americans' civil rights, privacy, and physical safety. Many companies comprise a multi-billion-dollar market of gathering, sharing, and selling Americans' location information. This includes data brokers selling U.S. persons' smartphone location data—ranging from aggregated data on building foot traffic to real-time, individually identified smartphone geolocations. Data brokers work with mobile apps to get this data. Massachusetts has an opportunity to become a nationwide leader in preventing these extraordinary privacy abuses.

Today, I will recommend that the Massachusetts legislature consider a bill on the table to address these challenges: H.357 / S. 148, or "An Act protecting reproductive health access, LGBTQ lives, religious liberty, and freedom of movement by banning the sale of cell phone location information." Passing a robust and appropriately scoped version of this bill would be a major step towards preventing these kinds of harms to individuals and to society.

In this written testimony, I describe how:

- There is a multi-billion-dollar market for collecting, aggregating, and selling individuals' location data, which primarily entails mobile apps directly gathering location data from consumers and then selling that data to data brokers, which in turn sell it to buyers.
- Location data is highly sensitive because (1) it allows an individual or organization to observe, follow, or even hunt down a specific person, (2) physical movements over time are highly unique to individuals, and (3) location data enables an individual or organization to infer additional information about a person based on their movements.
- The sale of location data threatens Americans' freedoms and civil rights. Law enforcement exploits the data brokerage ecosystem to purchase data about Americans, including their smartphone geolocations, without warrants, public disclosure, or robust oversight.
- The sale of location data threatens Americans' privacy by trafficking in the sale of data about individuals, without their knowledge, that allows others to follow and target them, is highly unique to them, and can reveal other sensitive data points—including religion, sexual orientation, health information, signs of marital strife, and financial status.
- The sale of location data threatens Americans' safety by enabling violent and abusive individuals to hunt down and stalk, harass, intimidate, assault, and even kill other people—as well as by potentially disclosing private information about vulnerable communities, including the LGBTQ+ community and people attempting to conceive a child, that could subsequently result in threats to those individuals.
- Claiming that consumers "consent" to the sale of their location data is a bogus, bad-faith argument that ignores the fact that consumers do not (and could not feasibly) read privacy policies and terms of service, companies make them deliberately hard to understand, and consumers cannot by themselves escape systemic surveillance and data brokerage problems.
- Massachusetts has an opportunity to be a national leader in protecting consumers' privacy and prohibiting the sale of smartphone geolocation data.

I would also refer the Committee and the legislature to my previous testimony to Congress on the data brokerage ecosystem, the types of data collected and sold about Americans, and the harms and risks to individuals, communities, and the country.[1]

Today, consumers with smartphones cannot escape the sale of their smartphone location data. This needs to change.

[1] Justin Sherman, "Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security," Written Testimony before the House Committee on Energy and Commerce: Subcommittee on Oversight and Investigations, April 19, 2023. https://d1dth6e84htgma.cloudfront.net/Sherman_Testimony_4_19_23_b40d947a8e.pdf?updated_at=2023-04-17T17:40:42.415Z; Justin Sherman, "Data Brokerage and Threats to U.S. Privacy and Security," Written Testimony before the Senate Committee on Finance: Subcommittee on Fiscal Responsibility and Economic Growth, Hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector," December 7, 2021. https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf.

**The Market for Location Data**

Data brokers are companies engaged in gathering, inferring, aggregating, and selling or licensing data about individuals. Alongside brokering health data, financial data, political data, and many other categories of information, the data broker industry sells Americans' location data.

In 2021, the location data market was by some estimates worth $12-16 billion globally.[2] The technology news outlet *The Markup* has published its own list of significant companies in the location data market, which include 1010Data, Acxiom, Babel Street, Foursquare, Gravy Analytics, Kochava, Placer.ai, SafeGraph, and Venntel as well as data broker clearinghouses like the Amazon Web Services Data Exchange and Datarade.[3] It is a dynamic industry. Location data brokers continue to crop up, and existing location data brokers keep expanding their collection of geolocation data, such as gathering more precise data and expanding into new countries.[4]

Companies primarily gather location data from individuals' smartphones. (A growing number of IoT wearable devices, Wi-Fi connected cars, and other technologies are gathering and transmitting location data, too.) Mobile apps may collect location data to perform ride-sharing services or display driving directions. They might also collect location data to display the weather for a user's current city; filter package delivery options to a given zip code; or just collect as much data as possible to then run advertisements targeted to subsets of users.

There is a wide range in how apps handle that location data once collected. In some cases, these apps and companies do not share the location information further. They use the data for their own internal purposes. However, many apps *do* share location data with third parties, including by selling data to data brokers and by sharing data with advertisers, which then sell the data to brokers. This enables or makes it even easier for companies, law enforcement organizations, and malicious individuals to then acquire and use the location data. It could also potentially enable foreign actors, such as the Chinese or Russian intelligence services, to acquire and exploit the location data.

The fact that many apps sell location data on their own users is an important point. Sometimes, when discussing the regulation of location data, policymakers only speak about third-party data brokers—companies that sell data on consumers with whom they have no direct business

---

[2] See, e.g., "Location Intelligence Market Size, Share & Trends Analysis Report By Vertical (BFSI, IT & Telecom), By Application (Remote Monitoring, Risk Management), By Service (System Integration, Consulting), And Segment Forecasts, 2023 – 2030," grandviewresearch.com, 2020, https://www.grandviewresearch.com/industry-analysis/location-intelligence-market#; "Location Analytics Market Value Will Be Reaching USD 55.14 Billion, By 2030, with a CAGR of 16.11%," globenewswire.com, August 24, 2022, https://www.globenewswire.com/en/news-release/2022/08/24/2504059/0/en/Location-Analytics-Market-Value-Will-Be-Reaching-USD-55-14-Billion-By-2030-with-a-CAGR-of-16-11.html.

[3] 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.

[4] See, e.g., Auren Hoffman, "SafeGraph 2022 Year in Review," safegraph.com, December 2022, https://www.safegraph.com/blog/2022-annual-report; Aaron, "Revolutionizing Geocodes: Foursquare's Geosummarizer Model Takes US POI Accuracy to New Heights," location.foursquare.com, June 6, 2023, https://location.foursquare.com/resources/blog/developer/revolutionizing-geocodes-foursquares-geosummarizer-model-takes-us-poi-accuracy-to-new-heights/.

relationship. But with location data, that overlooks the fact that mobile apps are a central enabler of this market: gathering location data directly from their own users and then selling it to brokers.[5]

Many data brokers that sell individuals' location data acquire that data from mobile applications on individuals' phones. Data brokers might pay a mobile app developer to use the broker's software development kit (SDK), or prepackaged app-building code, in the developer's app. The broker can then sit within the app and gather data directly on users, without them knowing. Users may download an app, grant the app some permissions on their devices, and never realize that the app developer is not the only one receiving those permissions (e.g., to a smartphone's GPS). Many apps that gather location data will also forego the data broker SDK path. Instead, these apps collect location data on their own users, and once the data is on the app developer's servers, the developer will sell it directly to a data broker through a server-to-server transfer. Users have no visibility into that practice. App stores do not presently have technical visibility into that transfer, either.

The financial incentives are clear: data brokers pay some app developers thousands, tens of thousands, or even hundreds of thousands of dollars for access to users' smartphone location data.[6] These apps enable the subsequent sale of Americans' location data on the open market by data brokers.

**Location Data's Sensitivity**

Location data is one of the most sensitive kinds of data that companies gather, infer, aggregate, sell, and share about U.S. individuals. This is for at least three reasons:

1. It allows an individual or organization to observe, follow, or even hunt down a specific person;
2. Physical movements over time are highly unique to individuals; and
3. Location data enables an individual or organization to infer additional information about a person based on their movements.

Location data enables an individual or organization to observe, follow, or even hunt down a specific person. Access to real-time smartphone location data reveals where an individual is at the exact, current moment in time. The precision of smartphone location data varies, depending on such factors as the density of buildings in an area, skyline view, and the app and operating system in question.[7] For example, some location data signals from smartphones could be around 30 meters

[5] For more discussion of this issue vis-à-vis defining data brokerage only as third-party activity, see: Justin Sherman, "GoodRx, Health Data Brokerage, and the Limits of HIPAA," Lawfare, March 6, 2023, https://www.lawfareblog.com/goodrx-health-data-brokerage-and-limits-hipaa; Justin Sherman, "Federal Privacy Rules Must Get 'Data Broker' Definitions Right," Lawfare, April 8, 2021, https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right.

[6] See, e.g., Tim Anderson, "Location tracking report: X-Mode SDK use much more widespread than first thought," *The Register*, February 3, 2021, https://www.theregister.com/2021/02/03/location_tracking_report_xmode_sdk/.

[7] Some location data brokers talk publicly about this precision question, in order to market their data as more precise than their competitors' data. See, e.g., Gravy Analytics, "How to Decipher Location Data Terms: 'Precision' vs. 'Accuracy,'" gravyanalytics.com, September 22, 2022, https://gravyanalytics.com/blog/decipher-location-data-terms-precision-vs-accuracy/; Chantal Tode, "Mobile location data is accurate up to 30 meters: report," marketingdive.com, undated (pre-2017), https://www.marketingdive.com/ex/mobilemarketer/cms/news/research/22928.html. See also, e.g., Kris Holt,

(~98 feet) to 70 meters (229 feet) off.[8] But other location data points can be incredibly precise, to the tune of several feet. Organizations can purchase this location data from the open market, in bulk, and then filter within the data to identify and track specific people—including by identifying individuals with the mobile advertising IDs (MAIDs) or device IDs that companies have assigned to them and their devices. Examples of this threat are discussed below. Historical location data or location data patterns can also enable organizations and individuals to follow or hunt down specific people by revealing travel patterns as well as regularly visited locations. An individual or organization with that data can learn where an individual usually is at a given time on a given day of the week, such as at their home, workplace, family member's home, child's school, or place of worship.

Additionally, location data is highly sensitive because physical movements over time are highly unique to individuals. Individuals' home address information is disturbingly public through "people search websites" that scrape public records and post the information online for search and sale; anyone with an internet connection can easily find where most Americans live. Therefore, any location dataset that includes an individual's home address information effectively reveals that individual's identity. In addition to concerns about identifiability and home addresses, there is extensive statistical and computer science research about the challenges with "anonymizing" location datasets given the uniqueness of movements to individuals and the ways in which datasets can be combined together to identify people.[9] Even new techniques to protect individuals' privacy in datasets (such as differential privacy)—which are important for first-party collector companies that responsibly use location data—have vulnerabilities and implementation challenges.[10] Data brokers selling location data are typically not concerned about these kinds of privacy risks. They may also sell to buyers that are only interested in accessing identifiable and/or real-time data.

Location data also enables an individual or organization to infer additional information about a person based on their movements. Companies and government organizations that buy individuals' smartphone location data can secretly watch as people visit medical facilities, mental health therapists, payday loan offices, divorce attorneys, child counselors, government buildings, military facilities, places of worship, LGBTQ+ bars, political demonstrations, their children's schools, and much, much more. These visits can in and of themselves reveal other sensitive data points about individuals such as religion, sexual orientation, health and mental health conditions, financial

---

"Android phone location data is about to get a lot more accurate," Engadget, March 22, 2022, https://www.engadget.com/snapdragon-qualcomm-location-accuracy-trimble-132442728.html.

[8] Florence Rodgerson, "How to improve your location accuracy with Roam.ai," roam.ai, May 20, 2021, https://www.roam.ai/blog/location-accuracy.

[9] Hui Zang and Jean Bolot, "Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study," *Mobicom '11*, September 19-23, 2011, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=efa8bf558b2cec1c0838f83e8879a6b787a58be4, 2; Vyes-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen, and Vincent D. Blondel, "Unique in the Crowd: The privacy bounds of human mobility," *Scientific Reports* 3, no. 1376 (2013), https://www.nature.com/articles/srep01376.pdf?pdf=button%20sticky; Huaxin Li, Haojin Zhu, Suguo Du, Xiaohui Liang, and Xuemin Shen, "Privacy Leakage of Location Sharing in Mobile Social Networks: Attacks and Defense," *IEEE Transactions on Dependable and Secure Computing* 15, no. 4 (July/August 2018): 646-660, https://ieeexplore.ieee.org/document/7556276.

[10] Fatima Zahra Errounda and Yan Liu, "An Analysis of Differential Privacy Research in Location Data," *2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity)* (2019): 53-60, https://ieeexplore.ieee.org/document/8819448, 1.

difficulty, and signs of marital strife. Multiple examples already demonstrate this threat to individuals' privacy, freedom, and well-being. In August 2022, the Federal Trade Commission (FTC) filed a lawsuit against location data broker Kochava and alleged in its complaint that it was collecting precise geolocation data and selling it in ways that enabled tracking of individuals'

> "movements to and from sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence shelters, or other at-risk populations, and addiction recovery."[11]

For example, the geolocation data "could show how long consumers stayed at [an addiction recovery center] and whether a consumer relapses and returns to a recovery center."[12] Data brokers have also secretly tracked Americans visiting reproductive healthcare clinics and made the data available for sale and targeting use.[13] Data brokers might not sell the raw, underlying geolocation data they gather from smartphones. But even location insights—such as pattern data identifying individuals' most-frequently visited locations—can expose additional, sensitive data points.

**Location Data Sales and Threats to Freedoms and Civil Rights**

The sale of Americans' location data, including by mobile apps and data brokers, enables civil rights abuses and threatens Americans' freedoms. It is a core American principle that the government should not be able to arbitrarily surveil U.S. persons without judicial oversight and other accountability mechanisms. But our laws about data are incredibly outdated and filled with loopholes. In cases where law enforcement would normally need a warrant to acquire data about an individual, it can simply purchase the data from data brokers without warrants, public disclosure, or robust oversight. Law enforcement agencies across the country currently engage in this practice to buy data on millions of Americans. That includes purchasing highly sensitive data on Americans' geolocations.

At the federal level, the Electronic Communications Privacy Act (ECPA) of 1986 (18 U.S.C. §§ 2510-2523) updated the 1968 Federal Wiretap Act to address law enforcement's interception of electronic communications.[14] ECPA was passed well before the advent of smartphones, the explosion of the data broker industry, and the pervasiveness of geolocation tracking. The law's shortcomings currently enable law enforcement to purchase otherwise-protected data without a warrant. The nonprofit Center for Democracy & Technology explains it succinctly:

---

[11] *U.S. Federal Trade Commission v. Kochava Inc.* (2022). Complaint for Permanent Injunction and Other Relief. United States District Court for the District of Idaho. https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf. 1-2.

[12] Ibid., 9.

[13] Joseph Cox, "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics," *VICE*, May 3, 2022, https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood; Justin Sherman, "The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics," *Lawfare*, September 19, 2022, https://www.lawfareblog.com/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics.

[14] U.S. Department of Justice Bureau of Justice Assistance, "Electronic Communications Privacy Act of 1986 (ECPA)," bja.ojp.gov, accessed May 26, 2023, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#vf4tzl.

> "If the government wishes to access customer information held by an RCS [Remote Computing Service] or ECS [Electronic Communication Service], ECPA provides a specific legal process that must be followed. The government can obtain subscriber information, such as name, address, and phone number, by issuing a subpoena under Section 2703(c)(2)."[15]

But ECPA "permits RCS and ECS providers *to voluntarily* provide non-content information to non-government third parties."[16] Hence, if the third parties "are not RCS or ECS providers, ECPA does not apply and accordingly does not prohibit them from selling or otherwise providing the information to the government."[17] In other words, instead of following a legal process to conduct surveillance on an American, law enforcement agencies can simply buy the data from data brokers without a warrant, public disclosure, or robust oversight. They are effectively buying their way around legal protections from government surveillance.

Today, law enforcement agencies exploit legal shortfalls and gaps to purchase U.S. persons' geolocation data. U.S. Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and the FBI have purchased location data on millions of Americans' devices.[18] For example, in August 2020, CPB spent $475,944.49 on a purchase of location data from data broker Venntel.[19] A more comprehensive set of documents released in July 2022 under a Freedom of Information Act (FOIA) request by the ACLU showed that the Department of Homeland Security has spent millions of dollars on Americans' location data in recent years.[20] Members of the public have little to no visibility into this practice. There are also few safeguards: law enforcement does not need a warrant to buy data from data brokers, and there is little evidence there is robust oversight over the use of these datasets within law enforcement agencies. Even years earlier, a 2008 study from the Berkeley Center for Law & Technology found that "there was almost no evidence of controls to prevent [law enforcement] agency employees from misusing the databases" they were purchasing from data brokers.[21]

---

[15] Carey Shenkman et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers* (Washington, D.C.: Center for Democracy & Technology, December 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf, 16.
[16] Ibid.
[17] Ibid.
[18] Joseph Cox, "CBP Bought 'Global' Location Data from Weather and Game Apps," *VICE*, October 6, 2020, https://www.vice.com/en/article/n7wakg/cbp-dhs-location-data-venntel-apps; Byron Tau and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement," *The Wall Street Journal*, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Joseph Cox, "How an ICE Contractor Tracks Phones Around the World," *VICE*, December 3, 2020, https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps; Ashley Belanger, "FBI finals admits to buying location data on Americans, horrifying experts," *Ars Technica*, March 9, 2023, https://arstechnica.com/tech-policy/2023/03/fbi-finally-admits-to-buying-location-data-on-americans-horrifying-experts/.
[19] "Order for Supplies or Services," contracting document for Venntel obtained by Joseph Cox, August 5, 2020, https://www.documentcloud.org/documents/7222542-CBP-Venntel-1, 4.
[20] Shreya Tewari and Fikayo Walter-Johnson, "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data," ACLU.org, July 18, 2022, https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data.
[21] Chris Jay Hoffnagle, "Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," Berkeley Center for Law & Technology, 2008,

The nonprofit Electronic Frontier Foundation has published research into data broker Fog Data Science and its sale of data to U.S. law enforcement. Fog Data Science's platform sold to law enforcement is called Fog Reveal. For less than $10,000 per year, state, county, and local police across the country can access "billions" of data points on "over 250 million" devices.[22] The EFF's investigation found, among others, that the broker's software enables police "to perform 'geofenced' device searches, i.e. a search for all devices in a specified region on a map, and then find all other locations those devices were at other times."[23] Fog Reveal also claims that the product only contains "anonymized" data but simultaneously offers features to "deanonymize data by revealing device advertising IDs, IP addresses, and other phone details."[24]

Documents obtained by EFF reveal additional details. For example, Fog Reveal supposedly sells location data updated every 24 hours[25] and gives purchasers the ability to search for location data at a specific place, date, and time.[26] It even provides the ability to look up location data based on a specific device ID[27] and tag devices for future monitoring.[28] Federal buyers of Fog Reveal data could view additional data about devices such as the type and version of a user's browser, the type and version of their operating system, the type and model of their device, and their last seen IP address.[29] Critically, the EFF also notes that it could not verify Fog Data Science's claims, there is reason for skepticism regarding the data broker's statements, and some agencies working with Fog have terminated their contracts.[30]

On the federal level, there is bipartisan support for tackling this problem. Democrats and Republicans have both endorsed the *Fourth Amendment Is Not for Sale Act* to tackle this threat to Americans' freedoms and civil rights.[31] At an April Congressional hearing at which I testified, there was likewise bipartisan support for closing these legal gaps and better protecting Americans' privacy from data brokers. Those discussions are still ongoing in Congress.

---

https://www.law.berkeley.edu/center-article/big-brothers-little-helpers-how-choicepoint-and-other-commercial-data-brokers-collect-process-and-package-your-data-for-law-enforcement/.

[22] Bennett Cyphers, "Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police," eff.org, August 31, 2022, https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police.

[23] Will Greenberg, "Fog Revealed: A Guided Tour of How Cops Can Browse Your Location Data," eff.org, August 31, 2022, https://www.eff.org/deeplinks/2022/08/fog-revealed-guided-tour-how-cops-can-browse-your-location-data.

[24] Ibid.

[25] Fog Data Science, "Fog Data Science Reveal Portal User Manual," obtained by Electronic Frontier Foundation, https://www.documentcloud.org/documents/22273670-fog-data-science-portal-users-manual, 4.

[26] Ibid., 19.

[27] Ibid., 18.

[28] Ibid., 24.

[29] Greenberg, "Fog Revealed: A Guided Tour of How Cops Can Browse Your Location Data."

[30] Cyphers, "Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police."

[31] Office of Senator Ron Wyden, "Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act," wyden.senate.gov, April 21, 2021, https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.

**Location Data Sales and Threats to Individuals' Privacy**

As discussed above, location data is highly sensitive because (1) it allows an individual or organization to observe, follow, or even hunt down a specific person, (2) physical movements over time are highly unique to individuals, and (3) location data enables an individual or organization to infer additional information about a person based on their movements. A company, website, app, or device gathering this data directly from individuals should already impose strong privacy, cybersecurity, and access controls around the data. However, the subsequent sale of the data on the open market is an extraordinary invasion of Americans' privacy. It is made even worse by the fact that data brokers sell location data about hundreds of millions of people without their knowledge and without substantial ability to mask the individuals in the dataset.

Data broker Kochava's aforementioned activity—quietly gathering smartphone location data on consumers' visits to medical facilities, places of religious worship, mental health facilities, addiction recovery centers, and domestic violence shelters—is extremely invasive. The company is digitally following people around as they live their lives and learning sensitive information about them in the process, in some cases information literally related to those people's mind and body. Likewise, data broker SafeGraph's tracking of individuals visiting reproductive health clinics invades the privacy of individuals in one of their most private, personal, and potentially vulnerable moments.[32] These and countless other examples of tracking and selling Americans' geolocation data amount to secretive surveillance that can reveal individuals' religions, medical conditions, sexual orientations, signs of marital strife, financial statuses, and many other intimate data points.

Individuals can also use brokered location data to inflict harm on other, specific people and populations of Americans. In 2019, the *New York Times* obtained a dataset from a location data company containing over 50 billion location pings from more than 12 million Americans' phones.[33] The journalists were able to identify individuals visiting the Playboy Mansion overnight and people traveling to celebrities' estates—all the way to "military officials with security clearances as they drove home at night" and "law enforcement officers as they took their kids to school."[34] They were able to infer additional data from the location dataset, including signs of failing marriages, indications of drug addiction, and visits to psychological facilities.[35] While the journalists were not doing this work for the purposes of harming the individuals, it would be all too easy for an individual with malicious intentions to similarly track Americans through brokered datasets. In another case, a nonprofit organization purchased location data covering 2018-2021 that originated from multiple gay dating and hookup apps, such as Grindr, and sifted through that location data to identify, track, and out a closeted priest.[36]

---

[32] Cox, "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics.
[33] Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times*, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.
[34] Ibid.
[35] Ibid.
[36] Michelle Boorstein and Heather Kelly, "Catholic group spent millions on app data that tracked gay priests," *The Washington Post*, March 9, 2023, https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/.

In 2015, a data broker headquartered and operated out of Massachusetts, Copley Advertising, was secretly tracking the phone locations of individuals visiting reproductive health clinics.[37] According to the broker's owner, it was exercising the ability to "set up a mobile geo fence around an area—Planned Parenthood clinic[s], hospitals, doctor's offices that perform abortions" and then run targeted advertisements to the individuals in those areas.[38] In Copley Advertising's case, this entailed tracking the phone locations of people visiting reproductive health clinics, selling targeted advertising access to those phones to anti-abortion groups, and then letting them run ads to women literally in the middle of visiting clinics in New York, Ohio, Virginia, Missouri, and Pennsylvania.[39] The owner of this Massachusetts-headquartered data broker even stated that he "can tag all the smartphones entering and leaving the nearly 700 Planned Parenthood clinics in the U.S."[40] While the data broker did not sell anti-abortion groups access to these devices in Massachusetts, the Massachusetts Attorney General argued that it was possible the broker would do so and that it would violate Massachusetts' Consumer Protection (Act Gen. L. c. 93A, § 2).[41] Copley Advertising and its owner denied any wrongdoing but voluntarily entered into an Assurance of Discontinuance with the Attorney General.[42]

The Massachusetts Attorney General took an important and privacy-protective action against an invasive, manipulative data broker activity—tracking people with geolocation data and targeting them at one of their most vulnerable moments, when they could be making life-or-death decisions about their health and even their family's health. Nonetheless, it only addressed one set of actions taken by one company. The rest of the location data brokerage industry is left largely untouched.

**Location Data Sales and Threats to Individuals' Safety**

The sale of Americans' geolocation data threatens their physical safety. Organizations and individuals intent on doing harm to specific people can easily do so with location datasets.

For decades, abusive individuals have purchased other kinds of location data—principally, home address information gathered and sold by "people search websites"—to hunt down and stalk, harass, intimidate, assault, and even murder other people. This kind of stalking and gendered violence predominantly impacts women as well as members of the LBGTQ+ community. In 1999, an abusive individual purchased information online about a woman named Amy Boyer.[43] He did so by looking her up on Docusearch, a people search website, and buying data about her employer, Social Security Number, date of birth, work address, and more.[44] This individual then hunted down Amy Boyer and murdered her.[45] Tragically, this story is all too familiar to those who study data brokers and, even more importantly, those who work with and support victims and survivors of

[37] Sherman, "The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics."
[38] *Commonwealth of Massachusetts* in the Matter of *Copley Advertising, LLC & John F. Flynn* (2017). https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2452&context=historical. 3.
[39] Ibid.
[40] Ibid., 4.
[41] Ibid.
[42] Ibid., 5.
[43] Electronic Privacy Information Center, "The Amy Boyer Case: Remsburg v. Docusearch," archive.epic.org, February 2003, https://archive.epic.org/privacy/boyer/.
[44] Ibid.
[45] Ibid.

stalking and gendered violence. Data about individuals' whereabouts, collected and sold by companies seeking a profit, is routinely exploited by abusive individuals to hurt others.[46] In the lawsuit brought against Docusearch following the murder of Amy Boyer, *Remsburg v. Docusearch* (2003), the court ruled in its opinion that "it is undisputed that stalkers, in seeking to locate and track a victim, sometimes use an investigator to obtain personal information about the victims" and that the threat of stalking and identity theft means "the risk of criminal conduct is sufficiently foreseeable that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."[47]

Government employees are even at risk. In 2020, a violent, misogynistic individual bought information online about New Jersey federal judge Esther Salas and her family. He then went to her home, shot her husband, and shot and killed her 20-year-old son.[48] That individual had also been compiling a "dossier" of information about United States Supreme Court Justice Sonia Sotomayor.[49] The resulting Daniel Anderl Judicial Security and Privacy Act, named after Esther Salas' son, was passed as part of Congress' National Defense Authorization Act (NDAA) for 2023[50] and received strong bipartisan support for introducing more protections for information publicly posted about federal judges. Members of Congress that co-sponsored the bill noted, among other things, that violent threats against judges "are made more dangerous by the public disclosure of sensitive information about judges and their immediate families" and that U.S. lawmakers must "optimize our nation's personal data sharing and privacy practices."[51]

Smartphone geolocation data is different from home address information, but both fall under the "location data" umbrella and pose significant risks to individuals' safety. The ability to follow individuals in real-time risks enabling a violent actor or malicious organization to follow and harm them. Using geolocation data to track or follow people over time enables individuals and organizations to develop insights into their movement behavior—such as bars and clubs frequented, children's schools visited, travel patterns for certain days of the week, and so on. This data can likewise be used to predict an individual's location at a certain point in time. It could also be used to identify the locations of co-workers, friends, family members, and other loved ones.

---

[46] See, e.g., Hearing before the House Committee on Energy & Commerce: Subcommittee on Oversight & Investigations, "Internet Data Brokers: Who Has Access to Your Private Records?," June 21-22 and September 29, 2006, https://www.govinfo.gov/content/pkg/CHRG-109hhrg31363/pdf/CHRG-109hhrg31363.pdf; Kaveh Waddell, "How FamilyTreeNow Makes Stalking Easy," *The Atlantic*, January 17, 2017, https://www.theatlantic.com/technology/archive/2017/01/the-webs-many-search-engines-for-your-personal-information/513323/; Adi Robertson, "Senators ask FTC to fight stalkers exploiting people search sites," *The Verge*, March 4, 2021, https://www.theverge.com/2021/3/4/22313613/ftc-senator-letter-stalking-abuse-data-broker-people-search-sites;

[47] *Remsburg v. Docusearch* (N.H. 2003). https://casetext.com/case/remsburg-v-docusearch-1. 6.

[48] Esther Salas, "My Son Was Killed Because I'm a Federal Judge," *The New York Times*, December 8, 2020, https://www.nytimes.com/2020/12/08/opinion/esther-salas-murder-federal-judges.html.

[49] CBS News, "Federal judge whose son was killed in attack says gunman targeted Sonia Sotomayor," cbsnews.com, February 19, 2021, https://www.cbsnews.com/news/esther-salas-sonia-sotomayor-60-minutes-2021-02-19/.

[50] S.2340. *Daniel Anderl Judicial Security and Privacy Act* (2021). https://www.congress.gov/bill/117th-congress/senate-bill/2340.

[51] Office of Dianne Feinstein, "Feinstein, Menendez, Booker, Sherrill, Colleagues Introduce Bipartisan Bill to Protect Privacy, Safety of Federal Judges and their Families," feinstein.senate.gov, July 14, 2021, https://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=4DF1C31C-85C1-4F82-B5C7-F3418B31277F.

Home address information, posted online by people search data brokers, could also be paired with smartphone geolocation datasets to identify individuals.

Further, location data can be used to infer information about people where the mere public disclosure of that information can result in harm to a person. The spread of anti-LGBTQ+ laws and the spread of anti-abortion laws in the United States, for example, mean that data revealing sexual orientation, gender identity, ability to conceive, and pregnancy status, among others, would constitute a serious violation of privacy if publicly disclosed and could result in other people potentially threatening those individuals' safety. This harm must be considered as well.

The aforementioned examples of (a) the *New York Times* tracking individual people within a large location dataset and (b) the anti-gay nonprofit purchasing data originating from gay dating apps (like Grindr) and filtering it down to one person underscore that organizations intent on doing harm to a person buried within a larger dataset can do so. Data brokers' compilation and sale of location data—as well as analysis of location data and sale of those insights, patterns, and other metadata—threatens individuals' safety, at scale.

**The Bogus Idea of "Consenting" to the Sale of Location Data**

Many data brokers, when asked about their data practices, will claim that Americans "consent" to the packaging and sale of their data (including smartphone location data). In particular, brokers will often point out that many apps, websites, and other companies collecting data will include clauses in their privacy policies and terms of service that refer to the possibility of that first-party collector sharing data on consumers. This is a bad-faith and patently ridiculous argument. Most consumers do not read privacy policies, and the burden of doing so is overwhelming.

Among others, a 2019 Pew Research Center survey found that 81% of Americans agree to privacy policies at least monthly, but that only 9% of Americans say they always read a privacy policy before agreeing to a company's terms and conditions.[52] A 2021 survey by Security.org found that 37% of people skim the documents, 35% don't read them at all, and 16% search for and read a few key parts of the documents;[53] only 11% say they fully read privacy policies before agreeing.[54] The information asymmetry facing consumers is also huge: a 2008 study calculated that if consumers wanted to read the privacy policies for the services they use, it would take each person an average of 244 hours a year.[55] As the authors put it, "the national opportunity cost for just the time to read policies is on the order of $781 billion" (and that was in 2008).[56] The *New York Times*, to give another example, examined 150 companies' privacy policies in 2019 and found that they were difficult to read (an "incomprehensible disaster," the article's title said), with many even more

[52] Brooke Auxier et. al, "Americans' attitudes and experiences with privacy policies and laws," Pew Research Center, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.
[53] Eric Griffith, "Everyone Wants Data Privacy, But No One Reads Privacy Agreements," *PC Magazine*, April 19, 2021, https://www.pcmag.com/news/everyone-wants-data-privacy-but-no-one-reads-privacy-agreements.
[54] Ibid.
[55] Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* (2008), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/, 17.
[56] Ibid., 2.

complex than the texts that doctors, lawyers, and other professionals must understand in their jobs.[57] I spend much of my time researching data privacy issues and data brokerage, and I do not have time to read every single line in every single privacy policy of every single application I use.

Further, this idea of "consent" is not fully informed. Most consumers do not understand and cannot be reasonably expected to understand how the data brokerage ecosystem operates. There are many companies gathering data on consumers through websites, mobile apps, and other products and services and then—with very little or no transparency—selling and sharing the data with other actors. An individual downloading a weather app with a built-in GPS feature has no reasonable expectation the app might share their location data with a data broker which then sells it to advertisers or to law enforcement. (The FTC took an enforcement action in this vein in 2013 against flashlight app Brightest Flashlight Free, which indicated to users that location data would only be used internally but in reality shared and sold the data with third parties.[58]) Moreover, even if consumers did understand how the data brokerage ecosystem operates, that is distinct from fully understanding its harms. Companies and law enforcement agencies are building or buying increasingly sophisticated analysis tools for location data. They can track Americans and infer information about them far beyond what most people would expect or understand is possible, and machine learning and artificial intelligence capabilities could make this problem even worse.

The term "consent" also suggests it is freely given, but this is not the case with data brokers gathering and selling Americans' data. Even if consumers did fully understand what was happening in the data brokerage ecosystem and how it could or does harm them, the focus on individuals distracts from the systemic problems at play. There are an immense amount of information and financial asymmetries stacked against consumers impacted by data brokerage. People are regularly forced to interact with data brokers, whether to get a new credit card, put in a deposit for an apartment, or apply for a loan; many insurance companies buy data on consumers, too. Whether or not individuals "consent" to data brokerage is not a question limited to merely using an app that has a privacy policy somewhere if their not-consenting means they cannot access housing, money, employment opportunities, and other essentials.

In the location data space, consumers with a smartphone cannot escape the sale of their location data. The vast majority of mobile apps do not permit users to reject device permission requests and still use the app. Consumers who do not permit an app to access their location data usually cannot use the app, full stop. It is an all-or-nothing decision. For consumers who do permit an app to access their location data, they have no control over where that data goes once the app collects it. As mentioned above, the app can turn around and sell that data on the open market, including to data brokers who then package and further sell it. Consumers will neither know about it nor have the power to stop it. And there is limited opportunity, under the current U.S. regulatory structure, for consumers to be protected by default against these practices, although the FTC has been engaged in enforcements of data brokerage that amounts to "unfair or deceptive acts or practices"

---

[57] Kevin Litman-Navarro, "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster," *The New York Times*, June 12, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[58] Cecilia Kang, "Flashlight app kept users in the dark about sharing location data: FTC," *The Washington Post*, December 5, 2013, https://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html.

under Section 5 of the FTC Act. All told, being forced to submit to the use and potential sale of location data or not use apps entirely is not "consent."

**Recommendations**

The Massachusetts legislature has an opportunity to become a nationwide leader in protecting its citizens' location data privacy and preventing these harmful surveillance and data broker activities. I recommend that the legislature consider passing a robust version of H.357 / S.148 to prohibit the sale of cell phone location information. This should be paired with the necessary investments in regulatory enforcement to ensure that privacy violations are detected, investigated, and penalized.

Thank you.