

Your Digital Footprint

An inventory of what governments, corporations, and total strangers hold about you

747

times a day your online activity and location are broadcast to advertisers

3,000

attributes one broker keeps on nearly every U.S. consumer, including you

272M

Social Security numbers leaked by one broker you never heard of

50B

face images scraped into Clearview AI's database, likely including yours

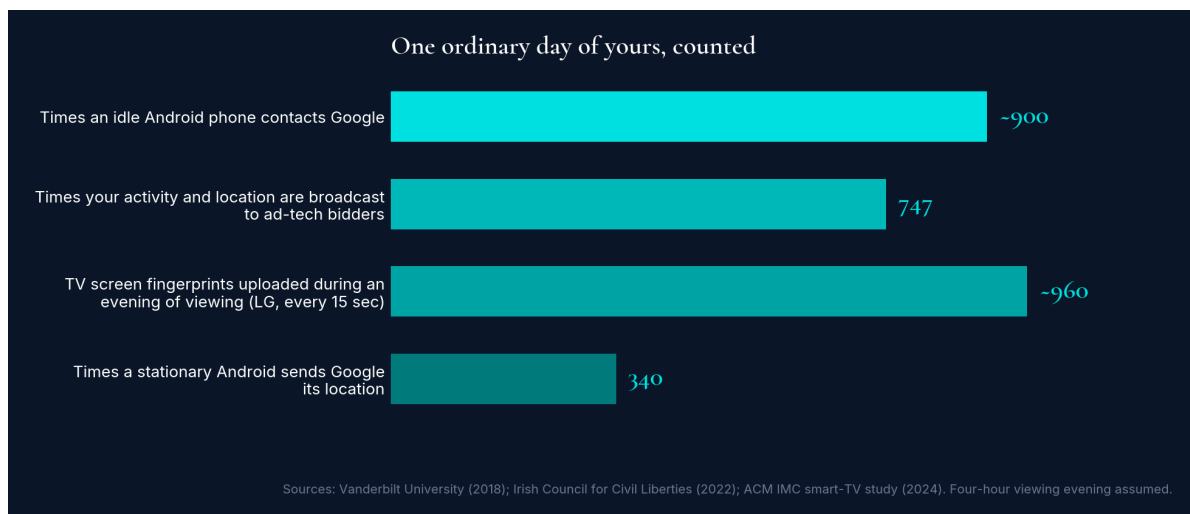
Sources: Irish Council for Civil Liberties (2022); FTC (2014); Atlas Data Privacy via Krebs on Security (2024); Weissman v. Clearview AI record.

START HERE

While you read this page

Reading this page takes about two minutes. In that time, your phone will check in with Google once or twice, even if it stays in your pocket. Your presence on this site has already been auctioned: the moment a page with ads loads, your location and interests go out to hundreds of bidding companies. If a smart TV is on in the room, it is photographing its own screen right now and uploading a fingerprint of whatever is playing, every 15 seconds on an LG, every minute on a Samsung.

None of that is hypothetical. Each number comes from a measurement study or a regulatory filing, and each one is about an ordinary person with default settings. Not a suspect, not a public figure. You.



This report walks through what exists about you, holder by holder: the brokers who built a file on you, the trail your phone leaves, the agencies that buy that trail, the devices in your house that report on you, the face and Social Security number you can never change, and the thin patchwork of law that is supposed to protect all of it.

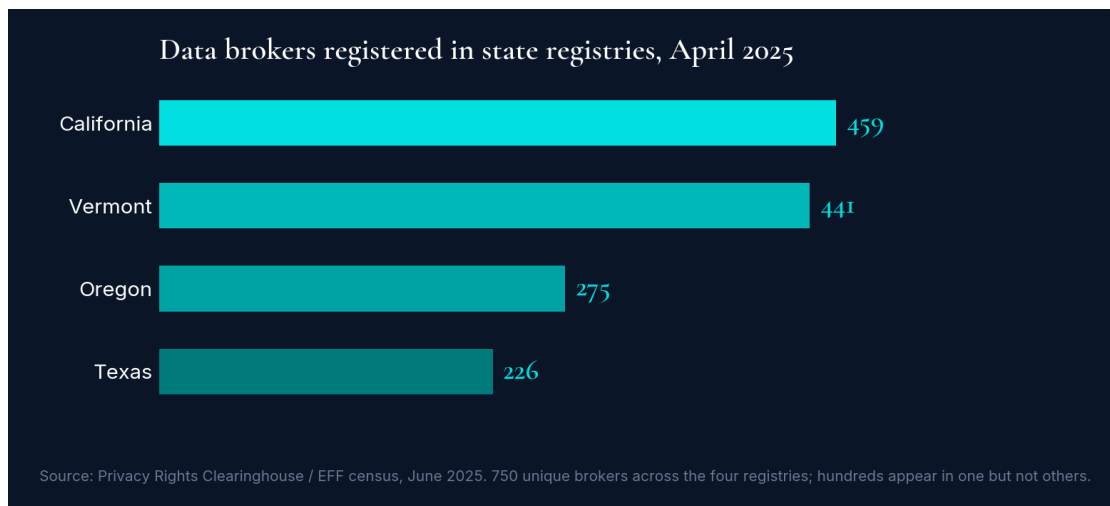
Your file

Somewhere in Arkansas, and in a few dozen other places, there is a file about you. You never opened an account. There is no login. You cannot read it. But it is for sale, and it is startlingly complete.

The Federal Trade Commission opened nine data brokers' books in 2014, firms like Acxiom, CoreLogic, and Datalogix, and found they held data on almost every U.S. household. One broker carried 3,000 separate attributes on nearly every American consumer. Another held 1.4 billion consumer transactions and 700 billion data elements. A third was adding three billion records a month. Your file draws from bankruptcy filings, voter rolls, warranty cards, purchase histories, and your web browsing. Seven of the nine brokers feed each other, so an entry in one file propagates to the rest.

The file is not just facts. It is judgments. The FTC found brokers sorting people into segments with names like **“Urban Scramble”** and **“Mobile Mixers”** (low-income Latino and Black consumers), **“Rural Everlasting”** (older, poor, less educated), and **“Diabetes Interest”** and **“Cholesterol Focus.”** If an algorithm ever quietly charged you more, showed you worse offers, or screened you out, a segment like these may be why.

Today, this is a market worth roughly \$300 to \$365 billion a year worldwide. It runs on people who have never heard of it. In fact, the FTC found consumers were generally unaware the industry existed. Only six states currently force brokers to register (California, Vermont, Texas, Oregon, Connecticut, and New Jersey). An April 2025 census found 750 distinct companies across four of those registries, and hundreds registered in one state while ignoring the others. The registered brokers are the visible ones.



Your location

Your phone's weather apps, game apps, and even prayer apps sell where you stand. Many of them carry advertising software that transmits precise GPS coordinates, and those coordinates flow to location brokers. In 2019, reporters at the New York Times obtained one broker's file of 50 billion location pings from 12

million phones. The data was nominally anonymous. It took the reporters minutes to attach names, following a phone from an office to a house, and they could do it for a Secret Service agent guarding the President.

What can a stranger learn from your trail? The broker SafeGraph sold a data package tracing everyone who visited any of Planned Parenthood's roughly 600 clinics. When researchers checked in August 2022, thirty-two other brokers were selling similar feeds. Your trips to a clinic, a church, a protest, a lawyer, a casino: each is a row in a product.

The FTC has spent four years suing its way through this market: X-Mode, InMarket, Avast (an antivirus company that sold its own customers' browsing histories), Mobilewalla (which kept the personal data it saw in ad auctions it lost on purpose), and Kochava, whose case ended a few weeks ago with a court order banning sales of sensitive location data without real consent. Every one of those cases is about data that came off phones like yours.

The customer you didn't expect: the government

In 2018, the Supreme Court ruled in *Carpenter v. United States* that the government needs a warrant to pull your location history from your phone carrier, because a location trail exposes, in the Court's words, "the privacies of life."

Federal agencies read that decision and went shopping instead. The record, agency by agency:

AGENCY	WHAT IT BOUGHT ABOUT YOU	THE PAPER TRAIL
Defense Intelligence Agency	Smartphone location data on Americans, held in a segregated database and queried with approval	Memo to Sen. Wyden, Jan. 2021: DIA "does not construe the Carpenter decision to require a judicial warrant" for purchased data
NSA	Internet metadata on wholly domestic traffic; can reveal the sites you visit and the apps you use	Written confirmation pried loose by Sen. Wyden, released Jan. 2024
IRS Criminal Investigation	Venntel's database of Americans' phone locations (2017 and 2018), searched without court orders	Wyden-Warren letter, Sept. 2020; Treasury watchdog warned the practice may be unconstitutional
CBP, ICE, Secret Service	Bulk app-derived location data: over \$2M to Venntel, nearly \$3M to Babel Street (CBP); \$649,467 (Secret Service)	DHS Inspector General, Sept. 2023: used without required privacy compliance
FBI and DEA	Venntel location services	Procurement records and FOIA litigation

Documented purchases of commercial data on Americans. Sources: ODNI declassified report (2023); Sen. Wyden releases; ACLU FOIA records; DHS OIG-23-61; USAspending.gov.

The intelligence community's own advisers said in a report written in 2022 and declassified in 2023 that commercially available information now "includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection." Because the agencies file it under "publicly available," it faces less internal regulation than data collected with a warrant. The same report noted that the exact kind of location data Carpenter protects is "openly for sale to the general public."

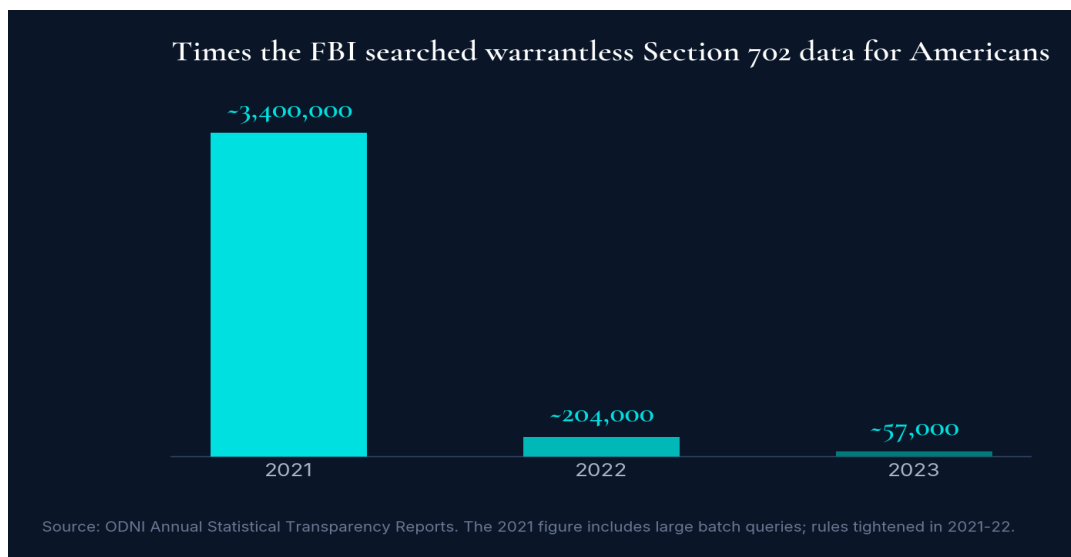
A bill to close this loophole, the Fourth Amendment Is Not For Sale Act, passed the House in April 2024 and died. As of this writing, no law stops an agency from buying what the Constitution would not let it collect.

THE WATCHERS

Your communications

If you have ever emailed, messaged, or called someone abroad, your side of the conversation may sit in an NSA database. FISA Section 702 lets the government collect foreign targets' communications without a warrant, and Americans on the other end are swept in as “incidental” collection. The government has never counted how many Americans are in the trove. Estimates run to the millions.

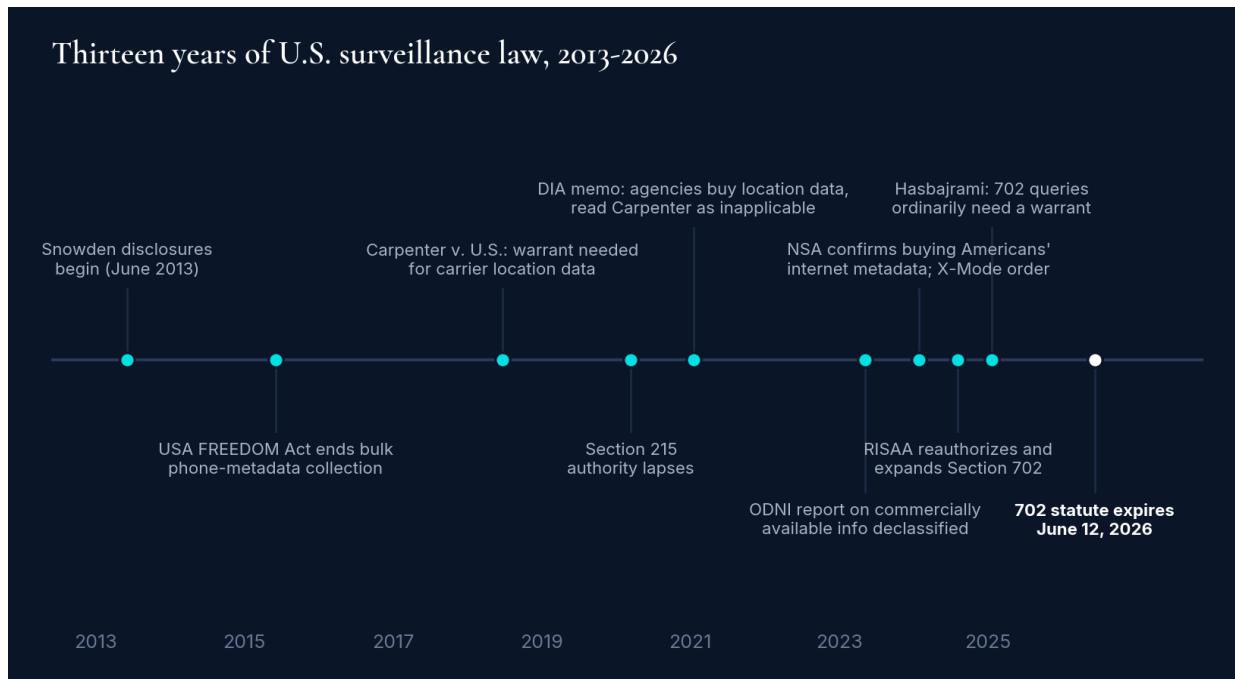
Additionally, the FBI can search that warrantless database for Americans by name, email, or phone number, including in ordinary criminal cases. In 2021 it ran roughly 3.4 million such searches.



Congress responded in April 2024 by renewing the program and widening it. The new law reaches “any other service provider who has access to equipment” that carries or stores communications, language critics summarized as “everyone who touches a router.” It did add guardrails on FBI searches requiring supervisor approval, a written factual basis, and special sign-off for searches on politicians and journalists. A warrant requirement failed on a 212 to 212 tie.

Then the program outran its own law. The statute hit its sunset on April 20, 2026; Congress passed two short patches, blew the June 12 deadline, and Section 702's statutory authority expired at midnight. Collection continues anyway, because court certifications approved in March 2026 stay valid for a year. A federal court, meanwhile, ruled in the Hasbajrami case that searching 702 data for an American ordinarily requires a warrant. Thirteen years after Snowden, the fight is still unsettled.

And all of that is the regulated part. Surveillance conducted overseas under Executive Order 12333, the authority behind programs that stored every call in and out of the Bahamas and let analysts watch internet activity live, has no judge and little Congress involved at all.

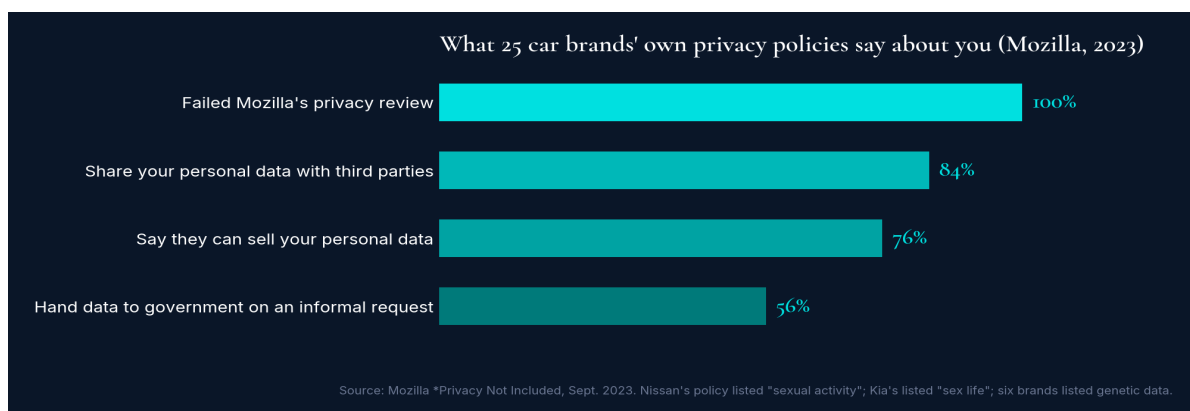


THE INFORMANTS

Your devices

Your television watches you. Samsung and LG, who sell about 41 percent of the world's smart TVs, both run Automatic Content Recognition: the TV periodically captures what is on its own screen and uploads a fingerprint to identify what you are watching. Researchers measured LG sets capturing the screen every 10 milliseconds and reporting every 15 seconds. It kept reporting when the TV was just an HDMI monitor for a laptop. The one good finding is that switching ACR off in settings actually stopped the traffic.

Your car is worse. Mozilla reviewed the privacy policies of 25 car brands in 2023 and failed every single one, the worst score of any product category it had ever tested. What the brands' own policies admit:



Ycar's maker probably shares your data, most likely reserves the right to sell it, and there is a better-than-even chance it will hand information to law enforcement on an informal request, no subpoena required. Nissan's policy claimed the right to collect data on your "sexual activity." Kia's said "sex life." Six brands mentioned your genetic information.

Your face

If a photo of your face has ever been on the public internet, assume it is in a police search tool. Clearview AI scraped what court filings describe as up to 50 billion images to build a face-matching product for law enforcement. The class in the resulting lawsuit was defined, in effect, as anyone whose face had been posted online.

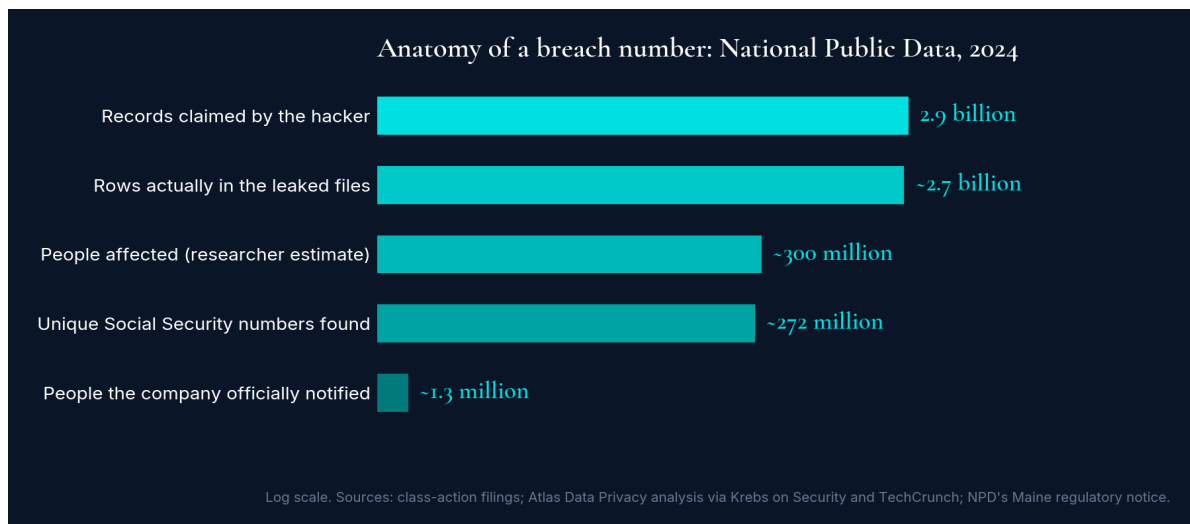
You have not been paid for it and probably never will be. A settlement approved in March 2025 would have given the class 23 percent of the company, valued around \$51.75 million, because a cash judgment would have bankrupted Clearview. On July 13, 2026, days before this report, an appeals court threw the settlement out. Seven years in, the scraping stands and no one has been compensated.

THE LEAKS

Your Social Security number

In April 2024, a hacker listed a database for sale claiming 2.9 billion records on Americans. The seller was not a bank or a tech giant. It was National Public Data, a background-check operation in Florida run essentially by one man, which had scraped public records into a product and stored the result badly. If your Social Security number was in it, you did not choose that company. It chose you.

Breach numbers inflate, and this one is a lesson in reading them:

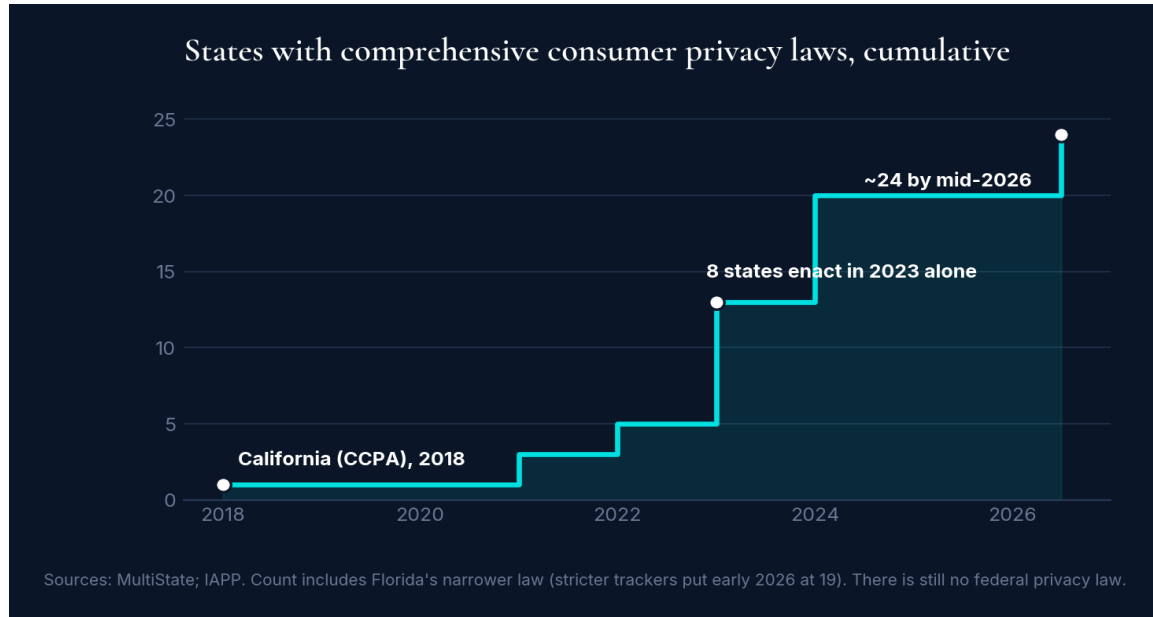


Researchers who parsed the leaked files counted about 272 million distinct Social Security numbers. The company formally notified about 1.3 million people, filed for bankruptcy on October 2, 2024, and was gone by December. The gap between those numbers is the industry's accountability, measured.

The stakes of a leaked identity are not abstract. In 1999, a stalker paid the broker Docusearch about \$20 for Amy Boyer's date of birth, \$45 for her Social Security number, and \$109 for her work address, which a subcontractor got by calling her and lying. He drove to that address and killed her. Her name briefly attached to a federal law restricting Social Security number sales. It was repealed before it took effect.

What stands between you and all this

No comprehensive federal privacy law. That is the headline after three decades of trying. What you actually have depends on your state:



About two dozen states now grant rights to see, delete, and stop the sale of your data. Most of those laws exempt “publicly available information,” which is exactly what people-search sites aggregate, so the industry that lists your address next to your relatives' names is largely untouched. California went furthest: its DROP platform opened in January 2026, and on August 1, 2026, every broker on the state registry must start honoring one-click deletion requests from Californians. Whether that works is the most important privacy experiment in the country right now.

Everything else is enforcement at the margins: the FTC picking off egregious brokers one consent order at a time, courts slowly extending the Fourth Amendment, and a Congress that has now let its own surveillance statute lapse rather than decide what the rules are.

BOTTOM LINE

What you can do, and what you can't

Turning off ACR stopped the TV studies' tracking cold. Denying app location permissions shrinks your trail at the source. An idle iPhone contacted its platform about 50 times less than an idle Android in the Vanderbilt measurements; defaults matter, and you can change many of them. If you live in a state with deletion rights, use them; if you are in California, DROP takes one request.

But be clear-eyed about the rest. You cannot opt out of the county property record, the voter file, or the breach of a broker you never chose. You cannot take your face off servers that scraped it years ago, and you cannot make an agency unbuy your location trail. The 747 daily broadcasts happen whether or not you are careless, because the architecture, not your behavior, produces them. That architecture was built in about

fifteen years, mostly without your knowledge and entirely without your signature. The file on you grows every day that the law leaves it profitable. Knowing what is in it is the place to start.

REFERENCES

Sources

Government and court documents

ODNI Senior Advisory Group Panel, Report on Commercially Available Information (Jan. 2022; declassified June 2023), dni.gov.
 FISA Amendments Act of 2008, Pub. L. 110-261; Reforming Intelligence and Securing America Act, Pub. L. 118-49 (2024); 50 U.S.C. § 1881(b)(4).
 Congressional Research Service reports R48592, LSB11148, and LSB11411 (Section 702; Hasbajrami).
 ODNI Annual Statistical Transparency Reports, 2022-2024 editions (FBI U.S.-person query counts).
 Carpenter v. United States, 585 U.S. 296 (2018).
 United States v. Hasbajrami (E.D.N.Y., ruling late 2024, unsealed early 2025).
 Weissman v. Clearview AI, No. 25-1673 (7th Cir., July 13, 2026), vacating settlement approval of March 20, 2025 (N.D. Ill.).
 DIA memo to Sen. Ron Wyden (Jan. 15, 2021); NSA correspondence released Jan. 25, 2024, wyden.senate.gov.
 Wyden-Warren letter to the Treasury Inspector General for Tax Administration (Sept. 2020).
 DHS Office of Inspector General, OIG-23-61 (Sept. 2023); USAspending.gov contract 70US0919C70090057.
 FTC, Data Brokers: A Call for Transparency and Accountability (May 2014).
 FTC actions: X-Mode/Outlogic (Jan. 2024), Avast (Feb. 2024), InMarket (May 2024), Mobilewalla (Dec. 2024), Kochava (final order, D. Idaho, June 25, 2026).
 California Privacy Protection Agency, Delete Act (SB 362) and DROP platform, privacy.ca.gov.

Studies and investigations

Irish Council for Civil Liberties, The Biggest Data Breach (2022): real-time-bidding broadcast measurements.
 D.C. Schmidt, Google Data Collection, Vanderbilt University (2018).
 Mozilla Foundation, *Privacy Not Included: Cars (Sept. 2023).
 ACM Internet Measurement Conference 2024: Automatic Content Recognition in Samsung and LG smart TVs.
 New York Times Privacy Project, Twelve Million Phones, One Dataset, Zero Privacy (Dec. 2019).
 Privacy Rights Clearinghouse and EFF, state data broker registry census (April 2025).
 Brennan Center for Justice, FISA Section 702 resource pages (2018-2026).
 ACLU, DHS location-data FOIA litigation and analysis (2022).
 Yale Law & Policy Review, End-Running Warrants (2023).
 The Business Research Company, Data Broker Market Report 2026; Mordor Intelligence, Data Broker Market.
 Krebs on Security; TechCrunch: National Public Data breach and bankruptcy coverage (2024).
 MultiState and IAPP state privacy law trackers (2026).
 Remsburg v. Docusearch, 149 N.H. 148 (2003).