March 24, 2026

VIA EMAIL & US POSTAL SERVICE

The Honorable Rand Paul
Senate Committee on Homeland Security and Government Affairs Committee
342 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Gary Peters
Senate Committee on Homeland Security and Government Affairs Committee
342 Dirksen Senate Office Building
Washington, DC 20510

The Honorable James Comer
House Committee on Oversight and Accountability
2157 Rayburn House Office Building
Washington, DC 20515

The Honorable Robert Garcia
House Committee on Oversight and Accountability
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Paul, Ranking Member Peters, Chairman Comer, and Ranking Member Garcia:

The Attorneys General of New Mexico, California, Colorado, Connecticut, Hawai'i, Illinois, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nevada, New Jersey, Oregon, Vermont, Virginia, and Washington urge Congress to take action to ensure that federal government agencies cannot use artificial intelligence technology to engage in mass surveillance of Americans. Such programs defy bedrock constitutional provisions that guard against federal government overreach, protect free speech, defend political activity, and secure our religious freedoms. Allowing federal agencies, whether directly or through contractors, to compile, analyze, and use large caches of information about intimate aspects of daily life of every American without limits, oversight, or accountability undermines the public's faith in our system of governance and is dangerous to our democratic institutions. In recent years, bills that would have modernized our statutory privacy and civil liberties protections have been introduced, but despite bipartisan support, failed to be enacted.[1] However, the recently introduced Government Surveillance Reform Act of 2026 includes provisions which, if passed along with regulations on private data collection and data broker practices, could begin to align our laws with contemporary technological capabilities. We

[1] *See, e.g.*, Security And Freedom Enhancement Act of 2024, S. 3961, 118th Cong. (2024); Government Surveillance Reform Act of 2023, H.R. 6262, 118th Cong. (2023); Government Surveillance Reform Act of 2023, S. 3234, 118th Cong. (2023); Fourth Amendment Is Not For Sale Act, S. 2576, 118th Cong. (2023); Protect Liberty and End Warrantless Surveillance Act of 2023, H.R. 6570, 118th Cong. (2023).

call on Congress to seize this opportunity and adopt legislation to stop the federal government's ability to evade existing legal limits on mass surveillance through the data broker loophole.

Federal Agencies' Purchase & Use of Commercial Datasets

Now more than any time in the past, Americans live online and on electronic devices. Private companies routinely compile troves of datapoints about individual and group behavior through the technology and artificial intelligence tools that power these platforms. Federal agencies have largely been unable to collect or review such quantities of information on the same scale as private sector actors, for practical reasons like limited resources and due to legal checks against state intrusion into our private lives. But in recent years we have witnessed the federal government move beyond mere development or purchase of surveillance technologies to requests for and procurement of large datasets from third-party data brokers and AI tools capable of mining these to extract information at the individual level.

Until last year, the FBI, DHS, ATF, SEC, and TSA had been purchasing travel data about Americans from the Airlines Reporting Corporation (ARC), a data broker owned by the major U.S. airlines. This data contained information about five billion ticketing records and was searchable by, among other variables, individual, giving these agencies access to information about every person's bookings, travel companions, and credit card information.[2] The program through which such data purchases were made, the Travel Intelligence Program (TIP), was shuttered after media reporting and pressure from Congressional members.[3] However, on March 6, 2026, the Secret Service published a Request for Information (RFI) on SAM.gov about "the existing capability or feasibility of creating an online investigative searching tool/application [that] would serve as a banking agency between airlines and travel agencies (such as Orbitz, Expedia, and Travelocity)."[4]

---

[2] Joseph Cox, *Airlines Sell 5 Billion Plane Ticket Records to the Government for Warrantless Searching,* 404 MEDIA (Sep. 15, 2025, at 9:14 MT), https://www.404media.co/airlines-sell-5-billion-plane-ticket-records-to-the-government-for-warrantless-searching/.

[3] Byron Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, THE WALL STREET JOURNAL (Feb. 7, 2020, at 7:30 ET), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Schuyler Mitchell, *DHS Wants to Build a System to Surveil Americans' Travel Records,* MOTHER JONES (Mar. 7, 2026), https://www.motherjones.com/politics/2026/03/dhs-wants-to-build-a-system-to-surveil-americans-travel-records/.

[4] U.S. SECRET SERVICE, REQUEST FOR INFORMATION - 3RD PARTY AIRLINE TRAVEL INFORMATION (2026), https://sam.gov/workspace/contract/opp/996f91f49cb54a4fb1d0882830d14104/view (last visited Mar. 23, 2026); *see also* U.S. SECRET SERVICE, DHS/USSS 3RD PARTY AIRLINE TRAVEL INFORMATION (RFI) 70US0926ES0001 QUESTIONS & RESPONSES (2026), https://sam.gov/workspace/contract/opp/996f91f49cb54a4fb1d0882830d14104/view (last visited Mar. 23, 2026) (access at "QAs" link).

Even the skeletal description in the RFI indicates that the app/tool in question, if acquired or accessed, would give the Secret Service the mass surveillance capabilities previously available through TIP that had alarmed the public and policymakers.

Meanwhile, DHS has, since at least 2017, been purchasing location data about individuals from data brokers who aggregate digital marketing data.[5] While some have defended the practice on the grounds that the data is "pseudonymized" – i.e., the tracked devices are labelled not by owner/username but by unique alphanumeric identifiers – data re-identification is an increasingly easy task, particularly with the sophistication of AI tools.[6] Just last week, both FBI Director Kash Patel and Defense Intelligence Agency Director James Adams confirmed that both of their agencies purchase location data about Americans from commercial sources for law enforcement purposes.[7]

In recent use cases, DHS has dropped any pretense of seeking pseudonymized datasets for specific, targeted law enforcement activities. Just last year, ICE issued a no-bid contract to a company called Penlink, obtaining licenses to use two of its location tracking systems powered by AI and sourced from millions of data points from commercial data brokers and social media accounts.[8] One system, Webloc, allows DHS to track the movement of specific devices within a given perimeter on a map, while the other, Tangles, "creates a sort-of daily life profile of the people it surveils."[9]

The federal government's ability to obtain much of this information in the ordinary course typically requires compliance with some legal process, whether through issuance of a subpoena, judicial review through warrant requirements, existence of individualized suspicion, or pre-acquisition public notice and creation of data protection protocols.

The data broker loophole to these safeguards allows for the *de facto* deployment of an artificial-intelligence-powered surveillance system, a disturbing escalation of the already unprecedented collection of personal data by public and private actors. Without additional statutory protections

---

[5] Tau and Hackman, *supra* note 3.
[6] *See, e.g.*, Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html; Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202 (2017).
[7] Alfred Ng, *FBI is Buying Data that Can Be Used to Track People, Patel Says*, POLITICO (Mar. 18, 2026, at 12:50 ET), https://www.politico.com/news/2026/03/18/fbi-buying-data-track-people-patel-00834080.
[8] Billal Rahman, *ICE Buying Americans' Location Data Under Scrutiny*, NEWSWEEK (Mar. 5, 2026, at 13:25 ET), https://www.newsweek.com/ice-buying-americans-location-data-under-scrutiny-11627381.
[9] Thomas Brewster, *ICE Just Spent Millions on Surveillance Tech Banned by Facebook*, FORBES (Sep. 18, 2025, at 18:16 ET), https://www.forbes.com/sites/thomasbrewster/2025/09/18/ice-spends-millions-on-social-media-spy-tech-banned-by-meta-facebook/.

and policies imposing limits, transparency, oversight, and accountability measures, we will fail to keep pace with the surveillance capabilities of our times.

The Data Brokerage Industry

The consumer datasets compiled, aggregated, analyzed, and sold by tech companies, advertisers, and data brokers disclose personal and highly specific information about individuals, such as commuting routines, family networks, medical treatment, political activity, religious practices, biometrics, and more. Most consumers are unaware of the breadth and scope of data these companies collect while they are using or purchasing apps, digital platforms, and devices with internet connectivity, let alone the amount or nature of *additional* personal information that can be deduced through AI technologies and cross-referenced datasets. A company's privacy and disclosure policies are often written in vague, complicated, and otherwise difficult to understand legal or technical terms. Opt-out opportunities are also misleading since they do not necessarily tell a consumer that the company also engages in data practices unaffected by this option and what those transactions entail. States have enacted laws and undertaken investigations into data brokers through the exercise of their traditional police powers to increase public awareness of industry practices and protect consumers and children. At the same time, the need for nationwide Congressional action to regulate the data industry is clear.

While federal legislation provides some remedies to individuals injured by data privacy breaches, a complementary federal framework governing front-end acquisition, AI-assisted analysis, and sale of consumer data does not exist. One small exception is the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA), which makes it unlawful for data brokers "to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual" to certain foreign countries or entities owned by them.[10] PADFAA's restrictions seek to reduce the risk of espionage and other threats to national security that arise when hostile actors have access to sensitive data that can be used for blackmail or to conduct mass surveillance.

However, these very same risks also exist when data brokers traffic such information to U.S. entities. A 2023 report by Duke University researchers demonstrated how one could easily purchase private information – including health, financial, and religious information – about active-duty personnel, their families, and veterans for as little as $.12 per record.[11] Relatedly, "audience segments" uploaded to one prominent U.S.-based marketing platform and available to other users – ostensibly for directed advertising purposes – included segments targeting consumers

[10] Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 815, 118th Cong. (2024).

[11] JUSTIN SHERMAN, ET AL., DATA BROKERS AND THE SALE OF DATA ON U.S. MILITARY PERSONNEL: RISKS TO PRIVACY, SAFETY, AND NATIONAL SECURITY 3 (Nov. 2023), https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.

based on certain health conditions and financial hardship, as well as the likelihood that they were "US government employees who are considered decision makers working specifically in the field of national security" and "individuals who work at companies registered with the State Department to manufacture and export defense-related technologies."[12] The availability and accessibility of such data poses risks to our service members' safety and well-being, as well as to our national security but falls outside PADFAA's scope.

The lack of regulation also threatens the safety of survivors of domestic violence, sexual assault, and stalking who participate in state-based Address Confidentiality Programs. Data brokers are under no nationwide obligation to exclude the substitute address (typically, a P.O. Box) from their collections; when combined with other behavioral data points, such information can identify the general location where a survivor lives, works, or shops. In December 2024, the FTC brought an enforcement action against Mobilewalla, a Georgia-based data broker that, among other things, digitally tracked residents of domestic violence shelters.[13] The company's business model involved purchasing and aggregating detailed, time-stamped location information for specific electronic devices, then selling licenses to third parties to use this refined data, which included raw location data outlining consumers' precise movements to "sensitive locations," such as "medical facilities, places of religious worship, places that offer services to the LGBTQ+ community, domestic abuse shelters, and welfare and homeless shelters."[14] The conditions of the FTC's final order against Mobilewalla in January 2025 include a prohibition against the company selling sensitive location information and against misrepresenting how it collects, uses, deletes, or discloses personal information.[15] Codifying these types of limits on actors in the data economy along with audit and other compliance assurance authority would better protect consumers who, right now, largely must wait for after-the-fact enforcement efforts. Some states have sought to fill this void by adopting data broker business registration and other transparency statutes, such as

[12] Dell Cameron and Dhruv Mehrotra, *Google Ad-Tech Users Can Target National Security 'Decision Makers' and People with Chronic Diseases*, WIRED (Feb. 28, 2025, at 7:21 ET), https://www.wired.com/story/google-dv360-banned-audience-segments-national-security/.
[13] Complaint, Mobilewalla, Inc., FTC Docket No. C-4811, https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallacomplaint.pdf.
[14] *Id.* at ¶¶ 19–26; *see also* FEDERAL TRADE COMMISSION, STATEMENT OF CHAIR LINA M. KHAN JOINED BY COMMISSIONER ALVARO M. BEDOYA & COMMISSIONER REBECCA KELLY SLAUGHTER IN THE MATTER OF MOBILEWALLA, INC. (Dec. 3, 2024), at 1–2, https://www.ftc.gov/system/files/ftc_gov/pdf/statement-khan-bedoya-slaughter-mobilewalla.pdf.
[15] *FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data*, FEDERAL TRADE COMMISSION (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data.

Vermont's Act 171,[16] Texas's Data Broker Act,[17] Oregon's HB 2502,[18] and California's Delete Act.[19] These and future such state laws serve a vital function responsive to the needs of individual states and their residents. However, creating a nationwide baseline for transparency, oversight, and accountability will better protect Americans, regardless of where they live or work.

Existing Statutory Protections

While some statutory protections like the E-Government Act and Privacy Act aim to limit the federal government's ability to obtain personally identifying information, their requirements often have been ignored by federal agencies, and additional protections could more fulsomely capture scenarios that arise today.

For instance, a 2023 DHS Inspector General report examined access purchased by CBP, ICE, and Secret Service from private companies to mobile device geolocation information that, among other things, provided information about the device's historical location and was pulled from a device's Advertising Identifiers (AdID or Mobile Advertising Identifier, MAID). AdIDs are alphanumeric identifiers tied to a particular device. While typically used by commercial enterprises for marketing purposes, the DHS entities acquired this information for various law enforcement intelligence operations. Through the cross-referencing of multiple datasets and use of AI tools, the identity of the individual or phone number associated with a device can be re-identified based on an AdID.[20]

---

[16] VT. STAT. ANN. tit. 9, §§ 2430, *et seq.* (West 2020) (requiring registration, fee payment, reports of data breaches per year, and mandatory disclosure of opt-out opportunities and whether they sell data of minors).
[17] TEX. BUS. & COM. CODE ANN. ch. 510 (requiring registration, fee payment, mandatory disclosure of data practices and opt-out procedures).
[18] OR. REV. STAT. § 646A.593 (requiring registration and fee payment).
[19] CAL. CIV. CODE §§ 1798.99.80, *et seq*. (requiring registration, fee payment, periodic reporting, and deletion of all personal information broker holds about residents who submit an opt-out to the California Privacy Protection Agency).
[20] For this reason, various states consider personally persistent device identifiers like the AdIDs to be "personal information" and therefore subject to state law privacy protections. *E.g.*, CAL. CIV. CODE § 1798.140(v)(1)(D) (defining personal information to include "[c]ommercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies"); WASH. REV. CODE § 19.373.010(18)(a) (defining personal information as "include[ing], but is not limited to, data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier"); TEX. BUS. & COM. CODE ANN. § 541.001 (defining personal data as "any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual"); CONN. GEN. STAT § 42-515(26) (defining personal data as "information that is linked or reasonably linkable to an

Even though it is possible to identify individual-level information through these databases, the Inspecter General's audit found that agencies had not complied with DHS privacy policies or the privacy impact assessments required by the E-Government Act of 2002 (P.L. 107-347) before compiling or maintaining such data.[21]

Like the E-Government Act, the Privacy Act of 1974 (5 U.S.C. 552a) functions largely as a prophylactic measure with public notice, data minimization, and information security requirements, subject to certain exemptions, including one for criminal law enforcement. Among other things, the Act requires agencies not subject to an exemption to publish a notice in the Federal Register of any system of records it intends to maintain, if that system contains any grouping of information about an individual that is retrievable by a personal identifier. The law also requires agencies to maintain only data "relevant and necessary" to carry out authorized purposes and prohibits disclosure of personal records to other agencies or individuals, but again subject to a criminal law enforcement exemption.[22]

The various requirements of the Privacy Act were intended to make it "legally impossible for the Federal Government in the future to put together anything resembling a '1984' personal dossier on a citizen," and to ensure "proper regard for privacy of the individual, confidentiality of data, and security of the system."[23] The criminal law exemption "was included by members who believed that [during the same 1975-1976 sessions], Congress would pass additional legislation specifically governing criminal justice databases," but these additional measures were not enacted.[24] Moreover, the Privacy Act was passed when the relevant law enforcement databases "*did not* amass records indiscriminately, but were based on suspicion" about specifically identified individuals, property, or transactions.[25] Nor did the federal government or private parties at the time have the ability to collect or analyze quantities of data on the scale since made possible by AI tools and modern technology.[26]

---

identified or identifiable individual"); KY. REV. STAT. ANN. § 367.3611 (19) (same); UTAH CODE ANN. § 13-61-101(24)(a) (same); VA. CODE ANN. § 59.1-575 (same).

[21] DHS OFFICE OF THE INSPECTOR GENERAL, CBP, ICE, AND SECRET SERVICE DID NOT ADHERE TO PRIVACY POLICIES OR DEVELOP SUFFICIENT POLICIES BEFORE PROCURING AND USING COMMERCIAL TELEMETRY DATA, OIG-23-61 (Sep. 23, 2023), https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf.

[22] Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 VA. L. REV. 1351, 1378–79 (2024).

[23] S. Comm. on Gov't Operations and H.R. Comm. on Gov't Operations, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974 – S. 3418 (Pub. L. No. 93-579), Source Book on Privacy at 884, 1322–23 (1976).

[24] *Friedman & Citron*, *supra* note 22, at 1379.

[25] *Id.*

[26] *Id*.

The Congress that adopted the Privacy Act was not faced with the factual scenarios we encounter today. Additional protections are warranted to safeguard against the type of surveillance that the federal government is now undertaking. When faced with a similar disconnect between law and technology in the past, Congress enacted the Electronic Communications Privacy Act of 1986 to ensure federal wiretap laws accounted for the ability to intercept electronic communications.[27] We urge our legislators to meet the moment once again and pass legislation responsive to our times.

Congressional Action

As our Supreme Court has said, "private [information], even in an area accessible to the public, may be constitutionally protected.[28] What is considered private evolves with what "society is prepared to recognize as 'reasonable.'"[29] The wholesale collection of precise location data Americans for every minute and intimate details of Americans' daily lives by the federal government is simply unreasonable. Although several states have enacted comprehensive privacy and other laws to regulate data brokers, they gather vast amounts of consumer personal data with limited federal oversight and regularly without consumer knowledge. The data harvested from our mobile devices, the platforms on which they operate, and the apps we use to ease our daily lives can give law enforcement "access to a category of information otherwise unknowable," limited only by the technology and policies of the private company that possesses the data.[30] We need reasoned, debated policy to set guardrails on what has become the data broker loophole to existing civil liberties and privacy law protections. Integration of artificial intelligence into our society presents complicated, thorny questions that should be debated in the public sphere, not the backrooms of private companies.

Congress must take action to stop federal agency efforts to procure, create, or implement mass domestic surveillance until we have controls in place. We are encouraged by recent demands for information sent by Congressmembers and Committees to federal officials for greater disclosure and transparency around this issue. These efforts must coincide with the passage of legislation that would, among other things, --

- Prohibit the federal government from purchasing sensitive personal data, geolocation information (including that associated with mobile advertising IDs (AdIDs or MAIDs) or vehicles), or web browsing history of Americans from data brokers;
- Require federal law enforcement to obtain judicial warrants before acquiring and/or searching Americans' web browsing data, search queries, and location information, as well as before using AI to identify data subjects;

[27] *See* Electronic Communications Privacy Act of 1986, H.R. 4952, 99th Cong. (1986).
[28] *Katz v. United States*, 389 U.S. 347, 351 (1967).
[29] *Id.* at 361 (Harlan, J., concurring).
[30] *Carpenter v. United States*, 585 U.S. 296, 312 (2018).

- Ensure federal intelligence agencies are unable to exploit foreign surveillance loopholes to engage in domestic surveillance;
- Require federal agencies to delete unlawfully collected data about private individuals and any algorithms trained or used to make high stakes decisions using such unlawfully collected data, and;
- Reasonably regulate private data brokers to improve transparency over their data collection, maintenance, analysis, sale, and disclosure practices, and to give consumers greater control over the data collected and sold about them. Such regulations should not preempt more robust state laws and regulations applicable to the collection, sharing, and sale of personal information.

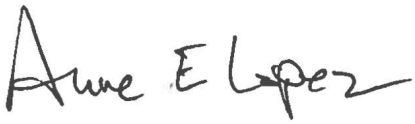
Technological progress cannot come at the expense of the people and our democracy. Congressional oversight and legislation responsive to this new era are essential.

Sincerely,

RAÚL TORREZ
New Mexico Attorney General

PHIL WEISER
Colorado Attorney General

ROB BONTA
California Attorney General



ANNE E. LOPEZ
Hawai'i Attorney General

WILLIAM TONG
Connecticut Attorney General

KWAME RAOUL
Illinois Attorney General

AARON M. FREY
Maine Attorney General

JENNIFER DAVENPORT
New Jersey Attorney General

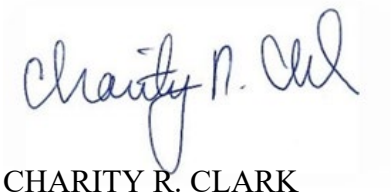
ANTHONY G. BROWN
Maryland Attorney General

AARON D. FORD
Nevada Attorney General

ANDREA JOY CAMPBELL
Massachusetts Attorney General

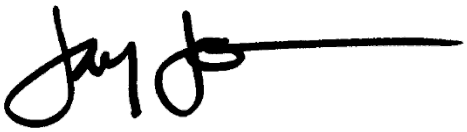
DAN RAYFIELD
Oregon Attorney General

DANA NESSEL
Michigan Attorney General



CHARITY R. CLARK
Vermont Attorney General

KEITH ELLISON
Minnesota Attorney General



JAY JONES
Virginia Attorney General

NICHOLAS W. BROWN
Washington Attorney General