

August 11, 2026
Chairman Chuck Grassley
Ranking Member Dick Durbin
Senate Committee on the Judiciary

Chairman Rand Paul
Ranking Member Gary Peters
Committee on Homeland Security and Government Affairs

**Close the Commercial Data Broker Loophole by Passing
the Fourth Amendment Is Not For Sale Act**

Dear Chairmen Grassley, Paul and Ranking Member Durbin, Peters:

We, the undersigned organizations, write to express our deep concern regarding recent reporting that the Department of Homeland Security and U.S. Immigration and Customs Enforcement have entered into a multi-year agreement with Thomson Reuters Special Services to access CLEAR, a commercial investigative platform capable of aggregating extensive personal information about millions of people in the United States.¹

The reporting highlights a problem that has continued to grow in recent years: federal agencies are purchasing access to commercially aggregated personal information that they could not otherwise obtain without judicial oversight.² This growing practice threatens to erode the protections guaranteed by the Fourth Amendment and underscores the urgent need for Congress to close the data broker loophole.

The Fourth Amendment was designed to prevent the government from conducting unreasonable searches of the American people.³ However, advances in the commercial surveillance marketplace have fundamentally altered that constitutional balance.⁴ Indeed, partial DHS legal analysis obtained under the Freedom of Information Act that shows the agency contorting itself to distinguish the cell phone location

¹ Caroline Haskins & Vittoria Elliott, *ICE Is Using Data Broker Tools to “Identify Unaccompanied Minors” and “Fraud”* WIRED, (July 17, 2026) <https://www.wired.com/story/ice-unaccompanied-minors-fraud-suspects-trss-contract/>; Olivia Bowden, *Canadian Government Urged to Block Thomson Reuters Data Deal with U.S. ICE*, Guardian (July 24, 2026) <https://www.theguardian.com/world/2026/jul/24/canada-government-mark-carney-block-data-sharing-deal-thomson-reuters-us-ice-avi-lewis>

² Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, Brennan Ctr. for Just. (Feb. 13, 2024), <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole>; Jude Joffe-Block, *Your Data Is Everywhere. The Government Is Buying It Without a Warrant*, NPR (Mar. 25, 2026), <https://www.npr.org/2026/03/25/nx-s1-5752369/ice-surveillance-data-brokers-congress-anthropic>; Anika Venkatesh & Lauren Yu, *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026), <https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access>.

³ U.S. Const. amend. IV.

⁴ *Carpenter v. United States*, 585 U.S. 296 (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

data that the Supreme Court held requires a warrant in *Carpenter v. United States*, from the equivalently sensitive and revealing location information to which the government is now purchasing access in bulk.⁵

Today, private companies collect, aggregate, analyze, and monetize extraordinary amounts of information about nearly every person in America.⁶ Rather than obtaining a warrant supported by probable cause, government agencies can purchase these comprehensive datasets using taxpayer dollars. According to former deputy director of the CIA Michael Morell, “[t]he information that is available commercially would kind of knock your socks off. If we collected it using traditional intelligence methods, it would be top secret sensitive. And you wouldn’t put it in a database; you’d keep it in a safe.”⁷

While this practice continues to grow across law enforcement and intelligence agencies, very little transparency exists as to the scope as to what data is being purchased and for what purposes.⁸ For instance, a report from the Office of the Director of National Intelligence found that while the intelligence community is collecting increasing amounts of commercially available information, it does not know how much it is collecting, what types, or what it is doing with the data.⁹

According to public reporting, CLEAR enables investigators to rapidly compile detailed profiles using information drawn from numerous public and proprietary sources, including addresses, telephone records, utility information, vehicle registrations, license plate records, social media activity, geolocation information, and other identifying data.¹⁰ Although individual records may independently exist in different places, aggregating them into searchable investigative dossiers dramatically expands government surveillance capabilities which further run the risk of being supercharged by the rapid growth and use of artificial intelligence by the federal government.

The contract may expressly contemplate use of the platform in investigations relating to voter fraud in addition to immigration fraud and national security.¹¹ This demonstrates the broad range of government functions now supported by commercially acquired surveillance tools. Without clear statutory guardrails, agencies across the federal government will continue to circumvent constitutional safeguards and expand their reliance on commercially purchased personal information.

The Constitution requires judicial oversight precisely because unchecked government access to personal information threatens liberty, democratic participation, and public trust. Therefore, we urge that you prioritize and advance the Fourth Amendment Is Not For Sale Act, which would prohibit government agencies from purchasing Americans’ sensitive information from commercial data brokers in

⁵ Anika Venkatesh & Lauren Yu, *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026), <https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access>.

⁶ See *supra* note 2.

⁷ Byron Tau, U.S. Spy Agencies Know Your Secrets. They Bought Them., Wall St. J. (Mar. 8, 2024).

⁸ See *supra* note 2.

⁹ Office of the Dir. of Nat’l Intel., *Senior Advisory Group, Panel on Commercially Available Information: Report to the Director of National Intelligence* 5–7 (Jan. 27, 2022), <https://www.govinfo.gov/content/pkg/GOVPUB-PREX28-PURL-gpo214640/pdf/GOVPUB-PREX28-PURL-gpo214640.pdf>

¹⁰ See *supra* note 1.

¹¹ Alex Barrientos, *ICE Plans \$125 Million Thomson Reuters Contract to Hunt “Voter Fraud”*, Yahoo News (July 15, 2026), <https://www.yahoo.com/news/politics/articles/ice-plans-125-million-thomson-184157977.html>

circumstances where a warrant or other legal process would otherwise be required.¹² Closing this loophole reaffirms the vital constitutional principle that the government should not be permitted to purchase their way around the Fourth Amendment.

In addition, we urge your Committees to:

- Hold oversight hearings examining federal agencies' acquisition and use of commercially available information obtained from data brokers.
- Require comprehensive transparency regarding federal contracts for commercially aggregated personal data, including the categories of information purchased, agencies involved, legal authorities relied upon, and oversight mechanisms governing their use.
- Examine whether existing procurement laws adequately protect constitutional rights when agencies acquire commercial surveillance capabilities.

Technological innovation has transformed the government's practical ability to learn intimate details about people's lives. Congress must ensure that constitutional protections evolve alongside those technological changes. The reports concerning Thomson Reuters' CLEAR platform are a reminder that the commercial surveillance economy has become deeply intertwined with government enforcement. The American people should not lose their Fourth Amendment protections simply because the government chooses to purchase information from a private company instead of obtaining it through a lawful judicial process.

We respectfully urge you to advance the Fourth Amendment Is Not For Sale Act and reaffirm that constitutional rights cannot be bought and sold.

Sincerely,

Public Citizen
American Civil Liberties
Union
Access Now
Advocacy for Principled
Action in Government
Asian Americans Advancing
Justice | AAJC
Autistic Women &
Nonbinary Network
Black Voters Matter Fund
Brennan Center for Justice at
NYU School of Law
Center for Democracy &
Technology
Common Cause

Consumer Federation of
America
Defending Rights & Dissent
Electronic Privacy
Information Center (EPIC)
Fiat Fiendum
Fight for the Future
Free Press Action
Government Information
Watch
Immigrant Legal Resource
Center (ILRC)
National Action Network

New America's Open
Technology Institute

Open MIC (Open Media and
Information Companies
Initiative)
Project On Government
Oversight
Restore The Fourth - Action
Secure Elections Network
Sikh American legal Defense
and Education Fund
TechEquity
The Leadership Conference
on Civil and Human Rights
UnidosUS
Vera Institute of Justice

¹² Protect Liberty and End Warrantless Surveillance Act of 2026, H.R. 7816, 119th Cong. (2026).

<https://www.congress.gov/bills/119th-congress/house-bill/7816/all-info>; Press Release, Sen. Ron Wyden, *Wyden, Paul and Bipartisan Senators Reintroduce the Fourth Amendment Is Not For Sale Act* (July 27, 2023), <https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-senators-reintroduce-the-fourth-amendment-is-not-for-sale-act>

