PROJECT ON GOVERNMENT OVERSIGHT

December 16, 2024

The Honorable Shalanda Young
Director
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Re: Request for Information on Federal Agency Collection, Processing, Maintenance, Use, Sharing, Dissemination, and Disposition of Commercially Available Information (CAI) Containing Personally Identifiable Information (PII)

Dear Director Young:

The Project On Government Oversight submits the following comment to the Office of Management and Budget (OMB) as it seeks to better understand federal agency collection and use of commercially available information (CAI) containing personally identifiable information. The Request for Information by OMB comes as part of its implementation of Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[1]

The Project On Government Oversight (POGO) was established in 1981 as a nonpartisan independent watchdog that investigates and exposes waste, corruption, and abuse of power. We advocate for essential reforms that create a more effective, ethical, and accountable federal government that safeguards constitutional principles.

The collection of CAI is a relatively new capability that can reach deeply into the lives of the American people.[2] The use of large data sets has expanded among federal agencies in recent years, with reports of agencies using the data in different ways.[3] Given the lack of transparency regarding the collection and use of this information, we have grave concerns that the unaccountable collection and use of CAI poses a threat to civil liberties and privacy rights.[4]

---

[1] "Request for Information: Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information," Office of Management and Budget, FR Doc 2024-23773, October 15, 2024, https://www.federalregister.gov/documents/2024/10/16/2024-23773/request-for-information-executive-branch-agency-handling-of-commercially-available-information; Executive Order No. 14110, 88 Fed. Reg. 71591 (October 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[2] Freddy Martinez, "Police Quietly Obtain Private Location Data with a Checkbook and not a Warrant," Project On Government Oversight, October 11, 2022, https://www.pogo.org/analysis/police-quietly-obtain-private-location-data-with-a-checkbook-and-not-a-warrant.

[3] Martinez, "Police Quietly Obtain Private Location Data with a Checkbook and not a Warrant" [see note 2].

[4] Don Bell, "We Built a Surveillance State. What Now?" Project On Government Oversight, August 20, 2024, https://www.pogo.org/analysis/we-built-a-surveillance-state-what-now.

This comment will outline our specific objections related to the federal government's current collection and use of CAI, particularly in supporting law enforcement functions. Specifically, we believe the government must cease purchasing individuals' data from data brokers, in circumvention of the Fourth Amendment's protection against unreasonable search and seizure, absent a warrant or appropriate court order to do so. This practice should be reined in immediately with the legislative and regulatory guardrails set forth at the end of this comment.

Overview

With the advent of more sophisticated online data collection tools and the pervasiveness of mobile applications, the capacity of businesses to collect highly detailed information on individuals has exploded into a multibillion-dollar sector, with forecasts estimating that the global industry will reach a value of nearly $562 billion by 2029.[5] However, data brokerage — the general practice of collecting, aggregating, selling, or sharing individuals' data — is virtually unregulated in U.S. law, at least on the domestic side.[6]

While the federal government has waded into the regulatory space with the passage of the Protecting Americans' Data from Foreign Adversaries Act of 2024, the act only restricts companies from selling "personally identifiable sensitive data" to foreign adversary countries or entities with significant ties to such a country.[7] The legislation is silent on data broker practices domestically. Most importantly, it does not address the use of data brokers to acquire and sell personally identifiable sensitive data domestically. To date, several states have passed data privacy laws, but they vary in the degree to which they protect CAI, and only a handful, such as Vermont, Oregon, California, and Texas, require data brokers to register.[8] This state-by-state approach creates a patchwork of accountability and is inadequate to address the growing problem.

In the absence of federal privacy law, the largest data brokers can collect, aggregate, and advertise for sale packages of data with thousands of data points on individuals. [9] According to the findings of a report by the Duke University Sanford Cyber Policy Program, 10 of the largest data brokers — most of which are headquartered in the U.S. — "openly and explicitly advertise data on millions of U.S. individuals, oftentimes advertising thousands or tens of thousands of sub-attributes on each of these individuals, ranging from demographic information to personal activities and life preferences (e.g., politics, travel, banking, healthcare, consumer goods and

---

[5] Mehdi Punjwani and Sierra Campbell, "Data Broker Statistics and Trends," *USA Today*, October 4, 2024, https://www.usatoday.com/money/blueprint/business/vpn/data-broker-statistics-and-trends/.

[6] Justin Sherman, "Data Brokers and Sensitive Data on U.S. Individuals," Duke Sanford Cyber Policy Program, 2021, 2, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf; Emile Ayoub and Elizabeth Goiten, "Closing the Data Broker Loophole," Brennan Center for Justice, February 14, 2024, https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

[7] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. Law. No. 118-50, 138. Stat. 933 (2024). https://www.congress.gov/bill/118th-congress/house-bill/815/text.

[8] Punjwani and Campbell, "Data Broker Statistics and Trends" [see note 5].

[9] There are models for a more consistent approach: In the European Union, although there is no legislation that speaks directly to data brokers, rules regarding individual data protection and sharing are covered by the General Data Protection Regulation (GDPR). See General Data Protection Regulation, Regulation (EU) 2016/679 (2018), https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en.

services)."[10]

As we have previously written, a person's phone can reveal incredibly intimate details of their life.[11] The information that applications collect through a phone goes beyond simple data. Location data can reveal your associations — which organizations you belong to, your political beliefs, and who you have relationships with. App history can reveal the medical conditions you or your family may have, whether you are pregnant, whether you are LGBTQ+, and the state of your mental health.[12]

For example, one of several data brokers that provide information to the federal government is LexisNexis.[13] LexisNexis on its website states it has the capacity to "identify relatives, associates and neighbors who may show up in photos or be mentioned in social media postings with a search of hundreds of networks and millions of sites on the open web," and draw connections "even when entities do not appear together in a public record" while also advertising the ability to "determine a person's current whereabouts" with drivers' license records.[14] The company earns millions each year with contracts that provide data services to federal agencies.[15] With this enormous and unchecked power, federal agencies, including federal law enforcement, have taken advantage of the absence of federal privacy legislation to collect enormous amounts of data on the American people.

In the law enforcement context, the purchase of CAI is effectively circumventing the Fourth Amendment.[16] Rather than seeking a warrant or court order for highly sensitive information about an individual, government agencies, the intelligence community, and law enforcement are choosing to pay third-party data brokers for the same information — with little oversight.[17]

There are numerous examples of this "data broker loophole" being exploited by federal agencies. In recent years, the IRS has subscribed to databases run by the broker Venntel, confirming to members of Congress its use of the product without a court order.[18] The subscription allowed the agency to potentially access a database of location data over 10,000 times, with Venntel's data coming from gaming and weather apps, among other sources.[19] The Centers for Disease Control

---

[10] Sherman, "Data Brokers and Sensitive Data on U.S. Individuals," 3 [see note 6].
[11] Bell, "We Built a Surveillance State. What Now?" [see note 4].
[12] Bell, "We Built a Surveillance State. What Now? [see note 4].
[13] "LexisNexis Risk Solutions Inc Recipient Profile," USASpending, data reported through FY 2024, https://www.usaspending.gov/recipient/b08f8773-1e62-248a-d212-05bf5257410e-C/latest.
[14] "LexID Advanced Analytics and SmartLinx Reports," LexisNexis, accessed November 25, 2024, https://www.lexisnexis.com/en-us/products/public-records/advanced-analytics.page; Sherman, "Data Brokers and Sensitive Data on U.S. Individuals," 4 [see note 6].
[15] Joseph Cox, "LexisNexis 'Virtual Crime Center' Makes Millions Selling to the Government," *Vice*, February 2, 2023, https://www.vice.com/en/article/lexisnexis-selling-data-government/.
[16] Bell, "We Built a Surveillance State. What Now?" [see note 4].
[17] Bell, "We Built a Surveillance State. What Now?" [see note 4].
[18] Letter from Ron Wyden and Elizabeth Warren, U.S. Senators, to J. Russell George, Treasury Inspector General for Tax Administration, about warrantless tracking of Americans' phones by the Internal Revenue Service's Criminal Investigation unit (IRS-CI), September 20, 2020, 1, https://www.wyden.senate.gov/imo/media/doc/092420%20Wyden%20Warren%20IRS%20letter.pdf.
[19] Internal Revenue Service contract No. NNG15SC77B for Venntel Mobile Intelligence Web-Based Subscription for 1 user (1 year), September 9, 2017, in Cox, "IRS Could Search Warrantless Location Database Over 10,000 Times," *Vice*, November 24, 2020, https://www.vice.com/en/article/irs-location-data-venntel-contract/; Lee Fang,

and Prevention purchased data that tracked millions of Americans' locations to follow travel patterns and analyze compliance with COVID-era stay at home orders.[20] Within the Department of Homeland Security, law enforcement components such as Customs and Border Protection and Immigration and Customs Enforcement have, without a warrant, spent millions of dollars to purchase hundreds of thousands of location data points on people residing in the U.S.[21]

Lack of Transparency

The ways in which federal agencies purchase and use CAI and exploit the data broker loophole also raise serious issues of transparency. This is a multifaceted issue, with concerns stemming from how taxpayer funds are being spent, how the decision-making process for acquiring CAI proceeds, how agencies are using the data being collected, and whether agencies are even following the law and basic policies that are often required to assess the privacy impact of an action before taking it. [22]

Just last year, a DHS Office of the Inspector General report found systemic failures within the Department of Homeland Security to follow internal policies on technology procurement and development of privacy impact assessments related to CAI.[23] It is unclear whether other agencies that collect CAI have standardized procedures for procurement and for how that data is used. This has led to abuses, as we will outline below. As we have written previously:

> There is tremendous secrecy around how much our government spends on data purchases, and how they actually use the data they collect. At the state and especially local level, you are unlikely to find a discussion on law enforcement data purchases and even less likely to find a line item in a law enforcement budget for data purchases. At the federal level, the scale and scope of data purchases could be hidden behind unnecessarily broad classifications that shield purchases from public scrutiny under the guise of protecting national security. To know we can all be surveilled at the most detailed level, without an explanation of why or how pervasive that surveillance is, is the antithesis of our constitutional order.[24]

Public transparency is essential to understanding the scope of the warrantless surveillance taking place, as well as the public cost for purchasing, analyzing, and acting upon the data collected.

"FBI expands ability to collect cellphone location data, monitor social media, recent contracts show," *Intercept*, June 24, 2020, https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/.

[20] Joseph Cox, "CDC Tracked Millions of Phones to See If Americans Followed COVID Lockdown Orders," *Vice*, May 3, 2022, https://www.vice.com/en/article/cdc-tracked-phones-location-data-curfews/.

[21] Shreya Tewari and Fikayo Walter-Johnson, "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data," American Civil Liberties Union, 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.

[22] Fang, "FBI expands ability to collect cellphone location data, monitor social media, recent contracts show" [see note 19].

[23] Maria Villegas Bravo, "DHS Disregards Internal Policies and Avoids Fourth Amendment Protections to Track Your Location," EPIC, February 8, 2024, https://epic.org/dhs-disregards-internal-policies-and-avoids-fourth-amendment-protections-to-track-your-location/.

[24] Bell, "We Built a Surveillance State. What Now?" [see note 4].

Targeting of Historically Marginalized Communities

As your own request for information notes from a discussion on the role of artificial intelligence in data collection and analysis: "The readout from the White House roundtable addresses that concern as well, noting that '[r]ecent advancements in artificial intelligence, attendees cautioned, have rapidly expanded data brokers' abilities to draw inferences about individuals' lifestyles, desires, and weaknesses, and are incentivizing rampant data collection to fuel their development.'"[25]

The rapid advancement in technology poses unique risks to historically marginalized communities, and we have already seen how the unaccountable collection of CAI has been used to target these communities. One of the most shocking abuses of purchasing CAI comes from the Department of Defense, which in 2020 was revealed to have purchased CAI from a broker that sourced user location data from Muslim Pro, a popular prayer app.[26] Immigration and Customs Enforcement has been found using private utility data to target immigrants.[27] And the FBI renegotiated contracts that provided access to cell phone data in June of 2020, at the height of nationwide racial justice protests.[28] With the ability of CAI to reach deeply into the associations, travel patterns, and intimate information of individuals, these kinds of violations could lead to additional targeting in the name of domestic or national security if not met with reforms.

There is a clear pattern of overstepped mandates and outright abuses within agencies that purchase CAI that contains personally identifiable information. To continue without an overarching set of requirements and guidelines that prohibit the excesses noted above and provide transparency, accountability, and oversight risks expanding mass warrantless surveillance, further threatening historically marginalized communities that have borne the brunt of disproportionate policing and surveillance in the past.[29]

The exploitation of the data broker loophole could become a more prevalent surveillance tactic, particularly if the power of the federal government is ever used as a tool for authoritarianism. Agency and law enforcement purchases and use of CAI could be further used to target individuals seeking reproductive or gender affirming care, "disfavored" groups that protest policy positions, or eventually entire communities based on their national origin or ethnicity.[30] With these risks, it is imperative that regulatory action takes place immediately to protect these

---

[25] "Request for Information: Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information" [see note 1].
[26] Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, November 16, 2020, https://www.vice.com/en/article/us-military-location-data-xmode-locate-x/.
[27] Drew Harwell, "ICE investigators used a private utility database covering millions to pursue immigration violations," *Washington Post*, February 26, 2021, https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/.
[28] Laura Hecht-Felella, "Federal Agencies Are Secretly Buying Consumer Data," Brennan Center For Justice, April 16, 2021, https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.
[29] Bell, "We Built a Surveillance State. What Now?" [see note 4].
[30] Don Bell, "Protest Under a Surveillance State Microscope," Project On Government Oversight, November 4, 2024, https://www.pogo.org/analysis/protest-under-a-surveillance-state-microscope; Caroline Haskins, "ICE Started Ramping Up Its Surveillance Arsenal Immediately After Donald Trump Won," *Wired*, November 13, 2024, https://www.wired.com/story/ice-surveillance-contracts-isap/.

communities from additional harm.

Recommendations for Action

It is clear that legislative and regulatory guardrails are urgently needed to protect civil liberties and privacy rights. The quickening pace of technological advancement combined with the expansion of CAI collection among agencies and a lack of regulation poses a serious risk to the American people.

As a result of bipartisan concern over the abuses coming from agencies related to the purchase of CAI, and the recognition of the need to stop the circumvention of constitutional safeguards, in the spring of 2024 a bipartisan majority of the U.S. House of Representatives passed the Fourth Amendment Is Not For Sale Act.

In the absence of Senate passage, there are immediate steps that federal agencies should implement to limit the government's purchase of CAI, ensure that practices do not disproportionately target marginalized communities, and provide needed transparency.

We recommend federal agencies take the following steps:

Implement protections to end the government's abuse of the data broker loophole.

- OMB should prohibit the purchase of CAI for law enforcement purposes without an appropriate court order.
- For non-law enforcement entities, CAI should only be acquired if it meets an appropriate privacy and civil liberties review and follows the policies of the agency making the acquisition.
- Regulation should require an agency to receive a court order if the agency seeks to compel data from telecommunications services, with the limited exceptions provided for in the Fourth Amendment Is Not For Sale Act, namely: express statutory authority to collect intelligence; collection of information of persons outside the United States; and foreign intelligence activity involving a foreign electronic communications system that does not violate the above listed exceptions.[31]

Create a prohibition on the use of CAI to target individuals and groups.

- Agencies must have a specific prohibition on any agency or law enforcement component of an agency purchasing CAI or using CAI to target individuals, organizations, or groups of people in a manner that is inconsistent with federal and state anti-discrimination laws. While there may be instances where CAI could be appropriately used to understand demographic trends, it should not be used to discriminate or target communities based on a protected characteristic.

Ensure public transparency regarding the collection, analysis, and use of CAI by agencies and law enforcement.

[31] Fourth Amendment Is not for Sale Act, H.R. 4639, 118th Cong., (2023), https://www.congress.gov/bill/118th-congress/house-bill/4639.

- Each agency should be required to issue a policy on the cases when CAI would be sought, how purchases are approved internally, and how CAI would be stored and destroyed. This will ensure that there is a standardized process for acquiring CAI and that agencies have policies in place to destroy the data once it has been used in a manner consistent with the acquisition's purpose.
- Agencies should require annual public reporting to the committees of jurisdiction in each congressional chamber on the amount of funds spent in the aggregate on CAI purchases, as well as an individual purchase breakdown and accounting of any CAI acquisition contract for the data itself or the purchase of a tool to disaggregate or analyze CAI. The reports should detail how CAI and CAI analysis technologies are used, how much contracts cost, and to whom contracts are being awarded.

Americans believe that the government is not doing enough to protect privacy. In a recent survey, 74% of Americans believed government was failing to protect their personal data online.[32] The reality is much worse, however. The unaccountable and unchecked ability of government agencies and law enforcement to purchase CAI, often for the purpose of circumventing Fourth Amendment warrant protections, puts privacy rights and civil liberties at risk.

We believe that OMB has the power to act now to eliminate the excesses of warrantless surveillance and move agencies toward more transparent, effective practices that will allow the use of CAI in more narrow instances and protect the rights of all.

We appreciate the opportunity to respond to your request for information.

Sincerely,

Don Bell
Policy Counsel, The Constitution Project
Project On Government Oversight

[32] Punjwani and Campbell, "Data Broker Statistics and Trends" [see note 5].