Joint Comment Regarding the Office of Management and Budget's Request for Information on Executive Branch Agency Handling of Commercially Available Information by the

Brennan Center for Justice at New York University School of Law
Demand Progress Education Fund
Electronic Privacy Information Center
Surveillance Technology Oversight Project
Advocacy for Principled Action in Government
Center for Democracy and Technology
Due Process Institute
Electronic Frontier Foundation
Free Press
Government Information Watch
New America's Open Technology Institute
Organization for Identity & Cultural Development
Privacy Rights Clearinghouse
Project for Privacy and Surveillance Accountability
Restore The Fourth
Secure Justice

December 16, 2024

I. Introduction

The Brennan Center for Justice at New York University School of Law (Brennan Center), the Demand Progress Education Fund (Demand Progress), the Electronic Privacy Information Center (EPIC), and the Surveillance Technology Oversight Project (S.T.O.P.), joined by the undersigned civil society organizations, submit these comments in response to the Office of Management and Budget (OMB)'s Request for Information on Executive Branch Agency Handling of Commercially Available Information (CAI) Containing Personally Identifiable Information.

The Brennan Center is a nonpartisan law and policy institute that works to reform, revitalize, and defend our country's systems of democracy and justice. Demand Progress is a charitable organization that educates its members and the general public about matters pertaining to the democratic nature of our nation's communications infrastructure and governance structures, and the impacts of corporate power over our economy and democracy. EPIC is a public interest research center based in Washington, D.C., established to protect privacy and human rights. S.T.O.P. is a New York-based civil rights and anti-surveillance group that advocates and litigates against discriminatory surveillance.

This comment highlights one dangerous aspect of agency handling of CAI that demands OMB's attention: law enforcement and intelligence agencies' access to and use of CAI in ways that evade legal requirements set forth in the Fourth Amendment and various privacy laws enacted by Congress.[1] Below, we discuss the Fourth Amendment doctrines and statutes that restrict the government surveillance at issue here, how the government is using CAI to circumvent those rules, the harms of this circumvention, and recommendations that OMB should implement to regulate these practices.

II. Current Government Practices Circumvent Constitutional and Statutory Protections and Impede Transparency and Oversight

A. [Q2-3, 14] Legal Restrictions on Government Collection of Personal Data

The Fourth Amendment and various federal statutes require government agencies to comply with legal process to obtain certain types of personal data on Americans. In those instances, Congress and/or the courts have weighed the government's need for personal information against the sensitivity of that information and have determined that the government should not have access without compulsory legal process.

1. Constitutional Standards

The Fourth Amendment requires the government to obtain a warrant to access information in which individuals have a "reasonable expectation of privacy."[2] For decades, however, courts interpreting the Fourth Amendment have held that people lose any expectation of privacy in information that they voluntarily disclose to others.[3] This is known as the third-party doctrine.

The third-party doctrine has proven untenable in today's world, where much of our information is stored or transmitted online and accessible to third parties that facilitate our digital transactions. Nearly every American carries a cell phone that tracks their every move; internet service providers store our search and browsing histories; and our documents are hosted by cloud service providers. Often, we disclose information to third-party providers without even realizing it.

In 2018, the Supreme Court began to chip away at this unworkable doctrine. In *Carpenter v. United States*, the Court examined the government's warrantless acquisition of a week's worth of

[1] For purposes of these comments, CAI does not include the following publicly available information: information that has been lawfully made available to the general public by (1) widely distributed media; (2) a website or online service made available to all members of the public, for free or for a fee, including where all members of the public can log in to the website or online service; (3) a disclosure to the general public that is required to be made by federal, state, or local law; or (4) federal, state, or local government records, if such information is collected, processed, retained, and transferred in accordance with any restrictions or terms of use placed on the information by the relevant government entity.

[2] See Katz v. United States, 389 U.S. 347 (1967).

[3] See U.S. v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

location information from a suspect's cell phone service provider.[4] Narrowing the third-party doctrine, the Court held that the government violated the Fourth Amendment by not obtaining a warrant for the cell phone location records. Individuals have a reasonable expectation of privacy in their location information despite sharing it with their cell phone providers because that data can reveal the most intimate details of their lives. The Supreme Court also found that the sharing of cell phone location information is not truly voluntary, given that the only alternative is to forgo cell phone use and — along with it — participation in modern life.

Although the Court declined to explain how its holding might be applied to other types of information, it made clear that the Fourth Amendment protects highly sensitive information conveyed through the use of essential technologies, and that the government must have a warrant to obtain such data. In doing so, the Court noted that a central aim of the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance."[5]

2. Statutory Standards

Before the Supreme Court's decision in *Carpenter*, Congress sought to place obstacles in the way of government surveillance by extending privacy protections to information held by third parties. An illustrative example is the Electronic Communications Privacy Act (ECPA), passed by Congress in 1986 to protect the privacy of Americans' communications in an era of new and emerging communications technologies.

As part of ECPA, the Stored Communications Act (SCA) restricts certain private companies — specifically, electronic communication service providers (i.e., phone and messaging services and social media platforms) and remote computing service providers (i.e., data storage and processing services) — from voluntarily revealing digital communications or information about those communications (e.g., metadata) to the government. Under the SCA, government entities must obtain a warrant, court order, or subpoena (depending on the type of records sought) in order to access both communications content and metadata. While the law is now outdated and fails to cover third-party data brokers or many app developers that collect and maintain personal data,[6] lawmakers who passed ECPA intended for it to evolve with new technologies "to ensure the continued vitality of the [F]ourth [A]mendment" and protection of Americans' privacy.[7]

Other types of sensitive data — such as health or financial information — are similarly protected by laws that restrict law enforcement's access to the information except for a strict set of permissible purposes or unless the government obtains the necessary subpoena, court order, or warrant

[4] See Carpenter v. United States, 585 U.S. 296 (2018).
[5] See *Carpenter,* 585 U.S. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
[6] Emile Ayoub and Elizabeth Goitein, "Closing the Data Broker Loophole," Brennan Center for Justice, February 13, 2024, https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.
[7] S. Comm. on the Judiciary, Electronic Communications Privacy Act of 1986, S. Rep. No. 99-541, at 5 (1986), https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf.

for the information.[8] These statutes bend toward a core principle: law enforcement and intelligence agencies cannot capitalize on new technology to conduct indiscriminate bulk surveillance or to collect information about individuals without judicial process.

B. [Q14] Role of Commercial Surveillance

While certain states have passed data privacy bills restricting data brokers,[9] the United States lacks a comprehensive federal privacy law that regulates the commercial collection and sale of personal data. Instead, it relies on a patchwork of statutes and regulations that apply to certain sectors or types of personal information.[10] Most of these laws and regulations are badly outdated, and the resulting gaps in coverage leave the majority of the data broker industry unregulated.

Today, CAI is available through commercial data sets that are increasingly intrusive, comprehensive, and cheap. The data broker industry profits from the extensive range of available information about individuals. This data includes, but is not limited to, detailed location histories; demographic information, including membership in legally protected groups, interests, affinities, and associations; and information about finances and wealth, property, healthcare, and internet search and browsing history. Data brokers and their clients claim that some or all of this data is "anonymized," but it can often be easily reidentified when combined with other information.[11]

---

[8] See, e.g., Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (1996), https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf (permitting health care providers to share certain information to law enforcement for limited purposes and requiring a court order for other information); 16 U.S.C. § 1681f and 16 U.S.C. § 1681b (Fair Credit Reporting Act provisions permitting consumer reporting agencies to share a narrow set of information to law enforcement agencies for limited purposes and requiring a court order for other information).

[9] For example, all states have a data breach law, see IT Governance USA, "Data Breach Notification Laws by State," accessed December 10, 2024, https://www.itgovernanceusa.com/data-breach-notification-laws; some have broader privacy bills, like the California Consumer Privacy Act, codified in Cal. Civ. Code § 1798.100 (Deering 2018).

[10] See generally, Rabia Bajwa and Farah Tasnur Meem, "Privacy's Peril: Unmasking the Unregulated Underground Market of Data Brokers, and the Suggested Framework," arXiv (October 6, 2024): 5, https://arxiv.org/pdf/2410.04606 (identifying U.S. privacy laws) For example, consumer information, financial data, and health data are all separately regulated. See Fair Credit Reporting Act, Pub. L. 91–508 § 601 (1970), https://www.govinfo.gov/content/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf, Gramm-Leach-Bliley Act, Pub. L. 106–102, 113 Stat. 1338 (1999), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6801&edition=prelim, Health Insurance Portability and Accountability Act, Pub. L. 104–191, 100 Stat. 2548 (1996), https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf, and Children's Online Privacy Protection Act, Pub. L. 105–277, 112 Stat. 2681-728 (1998), https://www.govinfo.gov/content/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap91.htm#:~:text=It%20is%20unlawful%20for%20an,(b)%20of%20this%20section.

[11] See Justin Sherman, "Big Data May Not Know Your Name. But It Knows Everything Else," *Wired*, December 19, 2021, https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/; Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?mod=article_inline.

Some categories of data are particularly revealing. Financial data brokers collect and sell data about individuals' net worth, debt, income, properties owned, vehicles owned, bank accounts, insurance policies, credit rating, and purchases;[12] this data can include sensitive information such as browsing and buying habits of prospective and current gun owners.[13] "People search" data brokers enable searches of individuals by name, address, phone number, or email, which can facilitate doxxing — the intentional publication of personal information with an intent to intimidate the target.[14] Health data brokers sell histories of prescription use, diagnoses, and medical devices.[15] Other data brokers sell information on people's interest in political organizations, political media figures, and politicians — including one data broker that claims it can predict voters' views on a range of political and social issues and identify Americans who hold specific beliefs.[16]

Many data brokers sell location data. This type of data is particularly intrusive, as the Supreme Court recognizes: a person's location history "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[17] Fysical and Safegraph, two data brokers offering location data, mapped people attending the 2017 presidential inauguration.[18] Another data broker allowed customers to use cell phone locations to learn who entered a mosque, who visited an abortion clinic, and where a police officer lived; one customer even tracked a juror from the courthouse parking lot to their home.[19] And in two recent investigations by the Federal Trade Commission, data brokers were found to have sold data to track and identify protesters, track Americans in military bases, and to help government agencies carry out immigration enforcement.[20]

---

[12] Steven Melendez and Alex Pasternack, "Here are the data brokers quietly buying and selling your personal information," *Fast Company*, March 2, 2019, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[13] See Corey G. Johnson, "Without Knowledge or Consent," *ProPublica*, October 24, 2024, https://www.propublica.org/article/gunmakers-owners-sensitive-personal-information-glock-remington-nssf; Patrick G. Eddington, "FISA and the Second Amendment: Gun Owners Beware," *RealClear Policy*, February 1, 2024, https://www.realclearpolicy.com/articles/2024/02/01/fisa_and_the_second_amendment_gun_owners_beware_1008782.html.

[14] Decca Muldowney, "So What the Hell Is Doxxing?," *ProPublica*, November 4, 2017, https://www.propublica.org/article/so-what-the-hell-is-doxxing.

[15] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, May 2014, https://utahpolicy.com/wp-content/uploads/2014/06/140527databrokerreport.pdf.

[16] See Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, Sanford School of Public Policy, Duke University, 2021, 7, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf; see also Alfred Ng, "Data broker offers access to voters likely to back Jan. 6 and right-wing militias," *Politico*, October 30, 2024, https://www.politico.com/news/2024/10/30/data-voters-political-violence-00186132; Emily Glazer and Patience Haggin, "Political Groups Track Protesters' Cellphone Data," *Wall Street Journal*, June 14, 2020, https://www.wsj.com/articles/how-political-groups-are-harvesting-data-from-protesters-11592156142.

[17] *Carpenter*, 585 U.S. at 2217.

[18] Valentino-DeVries et al., "Your Apps Know Where You Were Last Night."

[19] Brian Krebs, "The Global Surveillance Free-for-All in Mobile Ad Data," *Krebs on Security*, October 23, 2024, https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data/.

[20] Dell Cameron and Dhruv Mehrotra, "FTC Says Data Brokers Unlawfully Tracked Protesters and US Military Personnel," *Wired*, December 3, 2024, https://www.wired.com/story/ftc-mobilewalla-gravy-analytics-orders/.

Data brokers aggregate and sell every kind of information about people, taking advantage of the wide array of CAI to sell increasingly intrusive products. Data broker Thomson Reuters offers comprehensive "cradle-to-grave" dossiers on individuals through its online platform CLEAR, including names, photographs, criminal history, relatives, associates, financial information, and employment information.[21] The company offers its products to both private and public clients.[22] Data brokers aggregate information on billions of people for billions of dollars worldwide, and the industry is only expanding.[23] Perhaps most troubling, the unregulated data industry targets vulnerable populations, such as elderly Americans and women seeking reproductive health services.

C. [Q9, 14] Government Agencies' Purchase, Use, and Sharing of Commercially Available Information Circumvents Constitutional and Statutory Protections and Exploits the "Data Broker Loophole"

1. Agency Purchases

Over the past two decades, government agencies have increasingly turned to commercial entities like data brokers to quietly purchase access to Americans' geolocation information and other personal data without any legal process whatsoever.[24]

The known examples illustrate the range of agencies relying on the practice and the stakes involved. The military purchased location information from popular prayer apps to monitor religious communities.[25] DHS's Office of Intelligence and Analysis (I&A) used CAI procured through tools like LexisNexis to create dossiers on protesters.[26] State and local police departments followed suit, tracking protesters through the purchase of CAI.[27] Several other federal agencies have similarly purchased access to location information and other personal information — including the Federal Bureau of

---

[21] See Brooks v. Thomson Reuters, 2021 WL 3621837 (N.D. Cal. 2021) (Amended Complaint).
[22] See *Brooks*, 2021 WL 3621837 (Amended Complaint).
[23] Wolfie Christl, Cracked Labs, "Corporate Surveillance in Everyday Life," Institute for Critical Digital Culture, June 2017, https://crackedlabs.org/en/corporate-surveillance.
[24] See Carey Shenkman et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Center for Democracy & Technology, December 9, 2021, https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.
[25] Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
[26] See Spencer Reynolds and Faiza Patel, *A New Vision for Domestic Intelligence*, Brennan Center for Justice, March 30, 2023, https://www.brennancenter.org/our-work/policy-solutions/new-vision-domestic-intelligence; Office of Intelligence and Analysis, *Office of Intelligence and Analysis Operations in Portland*, U.S. Department of Homeland Security, April 20, 2021, https://www.wyden.senate.gov/imo/media/doc/I&A%20and%20OGC%20Portland%20Reports.pdf.
[27] Matt Cagle, "Facebook, Instagram and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color," ACLU of Southern California, October 11, 2016, https://www.aclusocal.org/en/news/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target; see also Bennett Cyphers, "How Law Enforcement Around the Country Buys Cell Phone Location Data Wholesale," Electronic Frontier Foundation, August 31, 2022, https://www.eff.org/deeplinks/2022/08/how-law-enforcement-around-country-buys-cell-phone-location-data-wholesale.

Investigation,[28] the Drug Enforcement Administration,[29] the National Security Agency,[30] and multiple components of the Department of Homeland Security.[31] Even the Internal Revenue Service has attempted to identify and track suspects by purchasing access to a commercial database that records smartphone location data.[32]

A June 2023 working group report on the intelligence community's use of CAI, which was partially declassified and released last year by the Office of the Director of National Intelligence (ODNI) (hereinafter, "Report to ODNI"), confirmed that intelligence agencies have been acquiring vast amounts of Americans' personal information from commercial entities, including location information and other sensitive data.[33] The Report to ODNI further noted that today, "in a way that far fewer Americans seem to understand, and even fewer of them can avoid, CAI 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."[34] Moreover, the report warned that intelligence agencies are not fully aware of what CAI they are acquiring and how they are using it.[35]

2. Data Sharing

Once one agency acquires data, it may be shared broadly among federal and state agencies. Information-sharing has historically been encouraged, including by OMB.[36] The federal Chief Data

[28] Byron Tau, "FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do." *Wall Street Journal*, March 10, 2023, https://www.wsj.com/articles/fbi-once-bought-mobile-phone-data-for-warrantless-tracking-other-agencies-still-do-ad65ebe9.

[29] Sara Morrison, "A surprising number of government agencies buy cellphone location data. Lawmakers want to know why," *Vox*, December 2, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel.

[30] Charlie Savage, "N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says," *New York Times*, January 25, 2024, https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html. The agency admitted that it purchased Americans' communications metadata from data brokers. Much like geolocation data, this information, when accumulated, can reveal intimate information like associations, habits, and beliefs. See ACLU v. Clapper, 785 F.3d 787 at 794 (S.D.N.Y. Aug. 26, 2013) (Declaration of Professor Edward W. Felten), https://s3.documentcloud.org/documents/781486/declaration-felten.pdf.

[31] Joseph V. Cuffari (Inspector General) to Alejandro Mayorkas (Secretary of Department of Homeland Security), Re: CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data, September 28, 2023, https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf.

[32] Byron Tau, "IRS Used Cellphone Location Data to Try to Find Suspects," *Wall Street Journal*, June 19, 2020, https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815.

[33] Office of the Director of National Intelligence Senior Advisory Group, *Panel on Commercially Available Information, Report to the Director of National Intelligence*, January 27, 2022 (hereinafter ODNI, *Report to ODNI*), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.

[34] ODNI, *Report to ODNI*.

[35] ODNI, *Report to ODNI*, 2, 21 (finding that the intelligence community "does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements" and "cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI").

[36] Jacob J. Lew (director, Office of Management and Budget), memorandum, Re: Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 20, 2000, at 1, https://www.whitehouse.gov/wp-content/uploads/2017/11/2001-M-01-05-Guidance-on-Inter-Agency-Sharing-of-Personal-Data-Protecting-Personal-Privacy.pdf.

Officer Council established a Data Sharing Working Group, which issued a comprehensive report in 2022 regarding the sharing of data across federal agencies.[37] Its recommendations included expediting data-sharing agreements, reinforcing the use of data.gov as a "government-wide metadata inventory," and broadly incentivizing data-sharing. The report also suggested developing "data-sharing centers of excellence within agencies."[38] While interagency cooperation — with appropriate limitations to avoid undue intrusions on privacy — can be essential to a well-functioning federal government, the consequence of an aggressive data-sharing approach is that if CAI is acquired by one agency, it may quickly spread across the federal government, and perhaps beyond.

Fusion centers are a particularly problematic example of information-sharing across federal agencies, as well as subnational government agencies.[39] Supported by DHS with funding, personnel, office space, and access to federal intelligence, fusion centers collect, analyze, and share intelligence from and among federal, state, and local law enforcement.[40] Many fusion centers also purchase access to data sets collected by data brokers like LexisNexis and credit reporting agencies like TransUnion.[41] DHS spends over $400 million a year on these fusion centers,[42] yet there is no evidence that they have contributed substantially to reducing or solving serious crime.[43] They do, however, promote unrestrained information sharing among government and private entities with minimal oversight or public accountability.[44]

3. Evasion of Legal Protections

Much of the CAI acquired by government agencies is, in theory, subject to statutory or constitutional privacy protections like ECPA and the Fourth Amendment. For example, the Supreme Court made clear in *Carpenter* that the government needs a warrant to obtain cell phone location records. Nevertheless, government agencies have made an end run around this warrant requirement by

---

[37] Nikolaos Ipiotis et al., Data Sharing Working Group, *Findings & Recommendations*, Federal Chief Data Officer Council, 2022, https://resources.data.gov/assets/documents/2021_DSWG_Recommendations_and_Findings_508.pdf.

[38] Ipiotis, *Findings & Recommendations*, 9.

[39] See U.S. Department of Homeland Security, "Fusion Centers," accessed December 8, 2024, https://www.dhs.gov/fusion-centers/; see also Michael German, Rachel Levinson-Waldman, and Kaylana Mueller-Hsia, *Ending Fusion Center Abuses*, Brennan Center for Justice, December 15, 2022, https://www.brennancenter.org/our-work/policy-solutions/ending-fusion-center-abuses.

[40] Office of the Director of National Intelligence, "Information Sharing Environment Guidance (ISE-G): Federal Resource Allocation Criteria (RAC)," June 3, 2011, https://www.hsdl.org/?view=&did=718364.

[41] See *Digital Dragnets: Examining the Government's Access to Your Personal Data, Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (2022), 7 (written statement of Sarah Lamdan, professor of law, City University of New York Law School), https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-LamdanS-20220719.pdf; Chris Cushing et al., *MIAC (Maine Information and Analysis Center) Shadow Report: Reporting on MIAC Auditing Processes Supplemental to the DPS Report*, April 1, 2022, 34, https://mainebeacon.com/wp-content/uploads/2022/03/MIAC-Shadow-Report.pdf.

[42] See total federal, state, and local budget in Department of Homeland Security, *2021 National Network of Fusion Centers Assessment: Summary of Findings*, 2021, https://www.dhs.gov/sites/default/files/2022-12/2021%20Fusion%20Centers%20Assessment%20Summary%20of%20Findings.pdf.

[43] German, Levinson-Waldman, and Mueller-Hsia, *Ending Fusion Center Abuses.*

[44] German, Levinson-Waldman, and Mueller-Hsia, *Ending Fusion Center Abuses.*

purchasing geolocation information from commercial data brokers. This practice violates the spirit of the Court's ruling, if not its letter. But agencies have interpreted *Carpenter* to apply only to the specific type of location data at issue in that case (i.e., historical cell-site location information), and only when the government *compels* companies to disclose information — not when private companies sell or voluntarily disclose information.

Agencies maintain that warrants are unnecessary even when the broker obtained the data through intrusive commercial surveillance without consumers' awareness.[45] In some cases, agencies make disingenuous claims that the customers consented to the selling of their data. In emails recently obtained by 404 Media, for example, the Secret Service argued that it could obtain location data harvested from mobile apps without a warrant because users had consented to such tracking by accepting an app's impenetrable terms of service.[46]

CAI can similarly be used to bypass statutory privacy protections. ECPA is a case in point. Although Congress passed ECPA in 1986 to protect the privacy of our digital communications content and metadata, the law has not been updated to reflect the modern world of mobile apps and commercial data brokers. As a result, even though ECPA prohibits telephone and internet service providers from providing certain sensitive customer information to government agencies without a court order, it places no restrictions on those companies selling the information to data brokers — or on data brokers selling it to government agencies. Government agencies have exploited this "data broker loophole" to purchase cell phone location information that would otherwise be protected under the law.

D. [Q3, 5-8, 14] Current Guidelines Regarding CAI Use are Opaque and Insufficient and Agencies Have Failed to Comply with Minimal Privacy Safeguards

Data brokers and other private entities that sell data often rely on opaque and even deceptive methods that are unknown to both the original consumers and the entities that obtain the CAI, including the federal government. Once the data is acquired by a government agency, additional layers of secrecy obscure the public's view into what data the agency is accessing and what happens to it thereafter — including how AI systems may be used to process, train on, transform, or interact with CAI. The public also has scant insight into how agency systems relying on CAI connect or interoperate with other systems and technologies within the agency, with other agencies, or with private sector contractors.

---

[45] See Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says," *New York Times*, January 22, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html; Hamed Aleaziz and Caroline Haskins, "DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People," *BuzzFeed News*, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

[46] Joseph Cox, "'FYI. A Warrant Isn't Needed': Secret Service Says You Agreed To Be Tracked With Location Data," *404 Media*, November 12, 2024, https://www.404media.co/fyi-a-warrant-isnt-needed-secret-service-says-you-agreed-to-be-tracked-with-location-data/.

While information regarding law enforcement and intelligence agencies' guidelines for handling CAI is limited, the little we do know reveals that agencies lack meaningful safeguards to protect privacy and civil liberties, have deficient policies that fall short of constitutional and statutory protections, have failed to keep track of their acquired data and use cases, and have failed to comply with their own privacy policies before acquiring and using CAI.

1. *Agencies' Routine Noncompliance with Privacy Impact Assessment (PIA) Requirements*

One reason why we know so little about agencies' CAI practices is that many agencies have been slow to comply with — or have simply violated — transparency and public disclosure obligations. Notably, agencies are required by the *E-Government Act of 2002* to conduct and publicly disclose privacy impact assessments (PIAs) for electronic information systems and collections that explain how they collect, use, and store personally identifiable information.[47] PIAs are intended to identify privacy risks, as well as mitigation strategies to ensure proper use and oversight. However, agencies often ignore their PIA requirements until a program is already implemented, if they conduct a PIA at all;[48] agencies may also withhold PIAs from the public on national security grounds.

For example, an investigation by DHS's Office of Inspector General into the handling of commercial telemetry data — which includes device location data — by CBP, ICE, and the Secret Service found that the agencies failed to adhere to DHS's privacy policies and the statutory requirement for agencies to obtain an approved PIA before acquiring such information.[49] Despite the significant risks to privacy regarding the handling of CAI, none of the components obtained an approved PIA before purchasing Americans' personal information. The OIG also found that the DHS components lacked sufficient policies and procedures governing their purchase and use of such data, including any supervisory review of officers' data queries.[50] As a result, the agencies failed to deter and detect abuse of that data, including an instance where a CBP employee used commercial data to track coworkers.[51]

The agencies' failures were so acute that OIG recommended that they discontinue their use of commercial telemetry data until they obtained an approved PIA and that DHS completely overhaul its department-wide privacy policy on the collection and use of commercial telemetry data.[52] In August 2024, CBP belatedly issued a PIA after nearly five years of purchasing the location information of

[47] E-Government Act of 2002, Pub. L. 107–347, § 208 (2002), https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.
[48] See Electronic Privacy Information Center, "Comments of the Electronic Privacy Information Center to the Office of Management and Budget, Request for Information: Privacy Impact Assessments," April 1, 2024, (hereinafter EPIC, "Comment to OMB"), https://epic.org/wp-content/uploads/2024/04/EPIC-Comment-to-OMB-re-PIAs-April-2024-with-Appendix.pdf.
[49] EPIC, "Comment to OMB."
[50] Cuffari to Mayorkas, Re: CBP, ICE, and Secret Service, 13.
[51] Cuffari to Mayorkas, Re: CBP, ICE, and Secret Service, 13.
[52] Cuffari to Mayorkas, Re: CBP, ICE, and Secret Service, 14–15.

millions of Americans.[53] The PIA illustrates the deficiencies in agencies' guidelines for handling CAI. For instance, the PIA acknowledges that individuals had no idea that their location data would be accessible to CBP via a CAI database, and that CBP failed to mitigate that privacy risk.[54]

2. *The Intelligence Community's Deficient Policies Fall Short of Constitutional and Statutory Protections*

Intelligence agencies have similarly deficient policies that are subject to even less public oversight and, as a result, diminished public accountability mechanisms. As mentioned above, the Report to ODNI concluded that the intelligence community is stockpiling massive amounts of CAI but does "not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements." It found that agencies lack meaningful safeguards to protect privacy and civil liberties, noting that most of the policies reviewed in the report focused on operational concerns rather than concerns about privacy, threats to civil liberties, and the sensitivity of information collected.[55] As a result, the report called on ODNI to first catalog the CAI that intelligence agencies acquire and to establish consistent guidelines for the intelligence community that promote transparency and meaningfully protect privacy and civil liberties.

The resulting ODNI policy rightly recognizes that agencies' acquisition and use of CAI puts Americans' privacy and civil liberties at risk. Despite the framework's laudable principles, however, it relies on subjective, discretionary, and exception-riddled standards that risk making it a box-checking exercise for agencies.[56] The framework also fails to prohibit intelligence agencies from purchasing information that would otherwise be subject to statutory or constitutional protections — more specifically, requirements to obtain a warrant, court order, or subpoena.[57]

Ultimately, these limited policies fall far short of the Framers' intent "to place obstacles in the way of a too permeating police surveillance."[58] As discussed above, Congress and the courts have already weighed the sensitivity of certain information against the government's need, and have determined that the government should not have access to such information without compulsory legal

---

[53] U.S. Department of Homeland Security, *Privacy Impact Assessment for the CBP Commercial Telemetry Data Evaluation*, August 20, 2024, (hereinafter DHS, *Privacy Impact Assessment for CBP*), https://www.dhs.gov/sites/default/files/2024-08/24_0812_priv_pia-cbp-080-commercial-telemetry.pdf.
[54] DHS, *Privacy Impact Assessment for CBP*, 12.
[55] ODNI, *Report to ODNI*, 26.
[56] Emile Ayoub, "The Intelligence Community's Policy on Commercially Available Data Falls Short," Brennan Center for Justice, September 12, 2024, https://www.brennancenter.org/our-work/analysis-opinion/intelligence-communitys-policy-commercially-available-data-falls-short; see also Office of the Director of National Intelligence, "ODNI Releases IC Policy Framework for Commercially Available Information," May 8, 2024, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3815-odni-releases-ic-policy-framework-for-commercially-available-information.
[57] Ayoub, "Intelligence Community's Policy"; see also ODNI, "ODNI Releases IC Policy Framework for Commercially Available Information."
[58] See Sherman, *Data Brokers and Sensitive Data*; see also *Carpenter,* 585 U.S. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

process. Yet agencies have chosen to replace the judgment of Congress and the courts with their own determinations that bypass legal process altogether.

III. Harms

A. [Q1, 9, 14] Commercially Available Information Can Be Abused to Cause Substantial Harms to Privacy, Civil Liberties, and National Security

1. Threats From Government Agencies to Privacy and Civil Liberties

Government agencies' practice of purchasing vast quantities of CAI that includes personal information poses threats to Americans' privacy and civil liberties. As noted above, such information, alone or combined, can reveal sensitive information about a person's movements, associations, habits, health conditions, and ideologies.[59]

The government can use this information to exercise its wide range of coercive powers over individuals, including the ability to arrest, imprison, deport, tax, fine, and even use lethal force. Unfettered government access to personal data without judicial oversight can also exacerbate existing biases in law enforcement and intelligence practices, permitting speculative investigations on the basis of conscious or subconscious biases — whether religious, ideological, racial, or ethnic — and the targeting of marginalized communities.[60] And the unrestrained access to such intimate information risks misuse or abuse by officers who can use it outside of their daily police work to stalk or harass romantic partners, neighbors, or business associates.[61]

Artificial intelligence (AI) exacerbates threats to privacy and civil liberties. AI tools make it easier to extract, re-identify, and infer sensitive information about people's identities, locations, ideologies, and habits — amplifying risks to Americans' privacy and freedoms of speech and association. Inaccurate CAI datasets incorporated into AI tools can also produce erroneous or flawed outcomes that can lead to wrongful arrests or misdirected investigations.[62]

In short, easy access to Americans' personal information by government agencies threatens privacy and the free exercise of fundamental rights, and these risks fall particularly heavily on members of marginalized groups.

---

[59] See ODNI, *Report to ODNI*; *Carpenter*, 585 U.S. 296; and United States v. Jones, 565 U.S. 400 (2012).

[60] Nicol Turner Lee and Caitlin Chin-Rothmann, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color,* Brookings Institution, April 12, 2022, https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

[61] See, e.g., Sadie Gurman and Eric Tucker, "Across US, police officers abuse confidential databases," Associated Press, September 28, 2016, https://apnews.com/general-news-699236946e3140659fff8a2362e16f43.

[62] See, e.g., Section II.B; Mona Rakibe, "The Significance of Data Quality in the World of Generative AI," Medium, June 21, 2023, https://medium.com/telmai1/the-significance-of-data-quality-in-the-world-of-generative-ai-5f84eb524299; and Kashmir Hill, "Wrongfully Accused by an Algorithm," *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

2. *Fueling A Harmful, Unregulated Industry*

The federal government's patronage of data brokers also causes harm indirectly, insofar as it supports an industry that generates a wide array of adverse impacts. Data brokers have compromised millions of Americans' sensitive information through data breaches, exposing unsuspecting individuals to harms like identity theft and fraud.[63] Malicious actors can also use data brokers to dox people, subjecting them to harassment, distress, and embarrassment.[64] Domestic abusers, stalkers, and other bad actors can use data from data brokers to stalk, harass, and commit violence.[65] Government employees and civil servants are not immune from this risk: data from data brokers can be used to identify and track jurors, law enforcement officers, and their family members.[66]

Moreover, data from data brokers can be used by foreign adversaries, threatening our national security.[67] Recent reporting by WIRED revealed that an American data broker collected and shared — as a free sample — more than 3 billion phone coordinates that expose the detailed movements of US military and intelligence workers abroad, information that could easily be used by a

[63] See, e.g., Brian Krebs, "NationalPublicData.com Hack Exposes a Nation's Data," *Krebs on Security*, August 15, 2024, https://krebsonsecurity.com/2024/08/nationalpublicdata-com-hack-exposes-a-nations-data/; Justin Sherman, "Data Brokers and Data Breaches," Sanford School of Public Policy, Duke University, September 27, 2022, https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/; and Brian Krebs, "Hacked Data Broker Accounts Fueled Phone COVID Loans, Unemployment Claims," *Krebs on Security*, August 6, 2020, https://krebsonsecurity.com/2020/08/hacked-data-broker-accounts-fueled-phony-covid-loans-unemployment-claims/.

[64] See, e.g., Joseph Cox and Emanuel Maiberg, "Fiverr Freelancers Offer to Dox Anyone With Powerful U.S. Data Tool," *404 Media*, July 2, 2024, https://www.404media.co/fiverr-freelancers-offer-to-dox-anyone-with-powerful-u-s-data-tool-tloxp/; and Joseph Cox, "The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15," *404 Media*, August 22, 2023, https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/.

[65] See, e.g., Letter from Amy Klobuchar and Lisa Murkowski, Senators in the U.S. Senate, to Hon. Rebecca K. Slaughter, Acting Chair, Federal Trade Commission, March 4, 2021, at 1, https://www.klobuchar.senate.gov/public/_cache/files/5/e/5e1e58a4-4b38-49e8-9a8b-37ea1604d9b9/A6F005737B2A977445475E4E0C2E3685.ftc-privacy-and-domestic-violence-letter-final---signed.pdf (explaining that "data brokers are publicizing the location and contact information of victims of domestic violence, sexual violence, and stalking"); and Mara Hvistendahl, "I Tried to Get My Name Off People-Search Sites. It Was Nearly Impossible.," Consumer Reports, August 20, 2020, https://www.consumerreports.org/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly--a0741114794/ (describing domestic abuse victim's effort to remove her information from data broker databases so that her abuser could not obtain it).

[66] See, e.g., Esther Salas, "My Son Was Killed Because I'm a Federal Judge," *New York Times*, December 8, 2020, https://www.nytimes.com/2020/12/08/opinion/esther-salas-murder-federal-judges.html (recounting instance in which litigant obtained federal judge's address from data broker and killed her son); and Joseph Cox, "Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics," *404 Media,* October 23, 2024, https://www.404media.co/inside-the-u-s-government-bought-tool-that-can-track-phones-at-abortion-clinics/ (explaining how data from data brokers could be used to identify and track jurors).

[67] See Michael German, "Letter Submitted to the CFPB on National Security Risks Posed by Data Brokers," Brennan Center for Justice, October 30, 2024, (hereinafter German, "CFPB Letter"), https://www.brennancenter.org/our-work/research-reports/letter-submitted-cfpb-national-security-risks-posed-data-brokers.

foreign enemy.[68] This followed a study by Duke University's Sanford School of Public Policy that surveyed the breadth of data collected and sold about military personnel and the risk that foreign actors could acquire the data to undermine our national security.[69]

To their credit, some agencies have begun to try to address these risks. The Federal Trade Commission recently brought enforcement actions against several data brokers, prohibiting their sales of certain location data.[70] The Consumer Financial Protection Bureau has proposed rulemaking that would restrict data brokers from sharing certain sensitive personal and financial information.[71] And the Department of Justice has proposed rulemaking that would restrict data brokers from sharing information with certain foreign adversaries.[72] As a whole, however, the federal government is voting with its checkbook. ICE spent almost $2.8 billion on data brokers' services from 2008 to 2021;[73] ICE is currently paying $22.1 million to LexisNexis for dossier service Accurint and $96 million to AI surveillance company Palantir;[74] the Department of Homeland Security pays Thomson Reuters $22.8

[68] Dhruv Mehrotra and Dell Cameron, "Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany, *Wired*, November 19, 2024, https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/.

[69] See Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel,* Sanford School of Public Policy, Duke University, November 2023, https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.

[70] See, e.g., Cameron and Mehrotra, "FTC Says Data Brokers Unlawfully"; Federal Trade Commission (hereinafter FTC), "FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data," January 9, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; FTC, "FTC Order Will Ban InMarket from Selling Precise Consumer Location Data," January 18, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data; FTC, "FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers; and FTC, "FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data.

[71] Consumer Financial Protection Bureau, "CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies," December 3, 2024, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-stop-data-brokers-from-selling-sensitive-personal-data-to-scammers-stalkers-and-spies/.

[72] Office of Public Affairs, "Justice Department Issues Comprehensive Proposed Rule Addressing National Security Risks Posed to U.S. Sensitive Data," U.S. Department of Justice, October 21, 2024, https://www.justice.gov/opa/pr/justice-department-issues-comprehensive-proposed-rule-addressing-national-security-risks.

[73] Georgetown Law Center on Privacy & Technology, *American Dragnet: Data-Driven Deportation in the 21st Century*, May 10, 2022, https://americandragnet.org/.

[74] Maurizio Guerrero, "Surveillance capitalism has taken over immigration enforcement—stifling dissent and sowing fear for profit," *Prism*, January 9, 2024, https://prismreports.org/2024/01/09/surveillance-capitalism-taken-over-immigration-enforcement/.

million for dossier service CLEAR;[75] and the FBI pays ZeroFox $14 million for protest monitoring.[76] As one of data brokers' largest customers, the government is massively subsidizing this harmful industry.

B. [Q1, 9, 14] Inaccurate Data Perpetuates Bias and Errors

Government agencies make decisions on a daily basis that affect people's lives. It is thus critical that the data on which agencies rely for all their activities — from individual adjudications to policymaking and research — be accurate. Yet CAI is often tainted with inaccuracies, such as names or addresses matched to the wrong people, typos, outdated data, incomplete records, and deliberately falsified information. Many data brokers also build and sell exhaustive dossiers that make inferences or predictions about individuals, sometimes using algorithmic tools or AI technologies to fill in missing information and infer attributes such as ethnicity, religion, or political views. Often these inferences are junk.[77] Finally, commercial data sets may be subject to manipulation by foreign adversaries, saboteurs, and cybercriminals, especially given the poor regulation of data brokers today.[78]

When the flawed CAI is shared with or sold to other entities, the data errors are perpetuated across domains and industries. The downstream consequences for Americans can be devastating, including lost job opportunities, rental housing denials, and rejected loan applications. Furthermore, these harms often manifest in ways that reflect and reinforce systematic biases and discrimination based on people's protected characteristics.[79]

Concerns about the risks of inaccurate or tainted data are magnified when the data is being used by law enforcement and intelligence agencies, which have unique coercive powers over individuals. Reliance by these agencies on inaccurate CAI can result in people being wrongfully investigated or even arrested. Moreover, some of the CAI relied on by these agencies may have been generated and/or collected as a result of corrupt, biased, or even unlawful surveillance or policing

---

[75] Contract Summary for Definitive Contract PIID 70CMSD21C00000002, awarded by U.S. Department of Homeland Security to Thomson Reuters Special Services LLC, USAspending, accessed December 9, 2024, https://www.usaspending.gov/award/CONT_AWD_70CMSD21C00000002_7012_-NONE-_-NONE-.

[76] Contract Summary for Definitive Contract PIID 15F06721P0002431, awarded by U.S. Department of Justice to CMA Technology Inc, USAspending, accessed December 11, 2024, https://www.usaspending.gov/award/CONT_AWD_15F06721P0002431_1549_-NONE-_-NONE-.

[77] See Suzanne Smalley, "'Junk Inferences' by Data Brokers Are a Problem for Consumers and the Industry Itself," *Record*, June 12, 2024, https://therecord.media/junk-inferences-data-brokers; see also Nico Neumann et al., "Data Deserts and Black Boxes: The Impact of Socio-Economic Status on Consumer Profiling," *Management Science* 70, no. 11 (January 2024): 8003, https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2023.4979?j (consumers "with higher incomes or living in affluent areas" are more likely to be profiled accurately by data brokers).

[78] See Heidy Khlaaf et al., "Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting," arXiv (October 18, 2024), https://doi.org/10.48550/arXiv.2410.14831.

[79] See Suzanne Smalley, "'Junk Inferences'"; see also Electronic Privacy Information Center, "Comments of the Electronic Privacy Information Center to the Consumer Financial Protection Bureau, Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information" July 14, 2023, https://epic.org/wp-content/uploads/2023/07/EPIC-CFPB-data-brokers-RFI-comments-071423.pdf.

practices and policies.[80] In such cases, agencies may be ingesting "dirty data" riddled with systemic biases or errors,[81] and using that flawed data to allocate agency resources, attempt to forecast criminal activity, determine targets of government surveillance, and engage in other governmental actions implicating people's lives and liberty.

Although some federal statutes governing privacy, such as the Fair Credit Reporting Act, provide a mechanism for correcting mistakes in certain types of personal data,[82] this patchwork of laws provides only very limited and incomplete relief. Companies that profit off our personal data generally operate with little oversight or accountability, in part because many consumers are not even aware of the pervasive corporate surveillance. Indeed, data brokers' financial incentives are to engage in stealth collection and sales of consumers' personal data and to obscure the flows of their data in the digital economy, not to proactively inform consumers about these practices and to provide clear recourse for them to correct errors or distortions.

IV. Remedies

For all the above reasons, we ask OMB to implement the following recommendations to ensure responsible federal agency use of CAI. Consistent with OMB's statutory authority to set policies for agencies' management of information resources, including CAI,[83] OMB should incorporate these recommendations into its policies and, as appropriate, OMB Circular No. A-130.

A. [Q2-3, 9-10, 14] Prohibit Exploitation of the Data Broker Loophole

The Fourth Amendment and certain privacy statutes place numerous restrictions on how and when the government can compel companies to provide data, but many of these restrictions can be circumvented through the simple expedient of patronizing a data broker. In practice, any law enforcement, military, or intelligence agency can purchase intimate information about anyone, at any time. Members of Congress introduced the Fourth Amendment Is Not For Sale Act to close this data broker loophole, but it has stalled in the Senate after passing in the House.

In the absence of a statutory prohibition on using CAI to circumvent Fourth Amendment protections, it is especially important for OMB to use its own statutory authorities to intervene and move federal agencies in the right direction. These OMB powers and responsibilities include its activities on behalf of the President during the annual budgetary process to guide and review agencies'

[80] See Rashida Richardson et al., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, And Justice," *NYU Law Review* 192 (February 2019), https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf.
[81] Richardson et al., "Dirty Data, Bad Predictions," at 192–233.
[82] Consumer Financial Protection Bureau, "A Summary of Your Rights Under the Fair Credit Reporting Act," accessed December 9, 2024, https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.
[83] See, e.g., 44 U.S.C. §3504(a); 5 U.S.C. §552a(v).

budget requests,[84] as well as its activities under the Office of Federal Procurement Policy Act[85] governing the government's acquisition of goods and services; the Paperwork Reduction Act[86] governing federal information policy, statistical policy, and privacy; the Chief Financial Officers (CFO) Act[87] addressing implementation of agencies' financial management policies; and the E-Government Act of 2002,[88] which requires PIAs as discussed and addresses the government's interactions with the public.

OMB should adopt a policy modeled on the Fourth Amendment Is Not for Sale Act,[89] and penalize any agency that violates this policy with recommendations of substantial budget cuts in the next budgetary cycle. The principle is simple: **law enforcement and intelligence agencies should be prohibited from obtaining CAI if the type of information to be acquired is subject to statutory or constitutional protections, unless the agencies first get the warrant, court order, or subpoena that would otherwise be required to collect that information.**

Other types of agencies will need to do their part as well. OMB should pass a parallel rule **preventing other agencies from purchasing and sharing CAI with law enforcement or intelligence agencies if those law enforcement or intelligence agencies would otherwise be required to get a court order to access the data**.

Of course, it will not be possible to apply this recommendation to the vast volume of CAI that has already been acquired. Instead, agencies should be required to apply minimization procedures in the form of restrictions on searches of that already-acquired data. Specifically, OMB should **restrict agency searches of CAI data that the agency has already acquired unless the agency obtains the warrant, court order, or subpoena that would be necessary, under this recommendation, to collect that information in the first instance.**

B. [Q2-3, 5-8, 12] Require More Oversight and Transparency

1. Improve Compliance with PIA Requirements

In addition to prohibiting agencies from exploiting the data broker loophole, we urge OMB to require meaningful oversight of, and transparency about, agencies' access and use of CAI. As a start,

[84] See, e.g., Congressional Research Service, "Office of Management and Budget (OMB): An Overview," June 22, 2023, https://crsreports.congress.gov/product/pdf/RS/RS21665.
[85] Codified at 41 U.S.C. § 1101.
[86] Codified at 44 U.S.C. § 3501 et seq.
[87] Codified at 31 U.S.C. § 901.
[88] Codified at 44 U.S.C. § 3602.
[89] Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Congress (2024) (as passed by House of Representatives), https://www.congress.gov/118/bills/hr4639/BILLS-118hr4639eh.pdf.

OMB should **strengthen existing requirements for agencies to conduct privacy impact assessments (PIA) and require more organized, consistent public disclosures of CAI uses.**[90]

PIAs can be a powerful mechanism for forcing agencies to weigh and minimize the privacy risks of a proposed agency action or program, including agency activities involving CAI. As noted above, however, agencies often complete the required assessment long after the project is established, provide inadequate information as a box-checking exercise, or fail to conduct a PIA at all.[91] In addition, the privacy threshold analysis (PTA) that agencies conduct to determine whether a PIA is warranted is generally not required to be disclosed to the public.

OMB should improve and expand the current PIA guidelines, with additional refinements addressing CAI uses, in order to ensure responsible agency use of CAI and to keep the public well-informed. To start, OMB should **require agencies complete PIAs *before* deploying a new information collection system or technology, not afterwards as a post-hoc justification**.

OMB should also **require a fuller analysis and public disclosure of the personally identifiable information involved with the new information system and details about the system itself**, including any relevant contracts and procurement decisions, the system's interoperability with other information systems, other entities' access to the data or system, and any formal or informal interagency or intergovernmental agreements governing CAI sharing or transfers between agencies or governments. Agencies should also be required to include in their PIAs a listing of any third-party contractors and the CAI that is sourced from them and incorporated into governmental systems. **The PTA should be released as well**.

Given that meaningful disclosures about agencies' use of CAI depends heavily on robust agency PIAs, OMB should **mandate more effective public access to PIAs**. OMB can make it easier for the public to find and view PIAs by either creating a user-friendly, centralized repository of the entire universe of agency PIAs or requiring agencies to publish all their PIAs online in a consistent, organized format.[92]

2. Reform Procurement Policies

OMB should **specify that contracts to procure or access CAI may not contain non-disclosure provisions masking the source of data used by law enforcement or intelligence**

[90] The Leadership Conference on Civil and Human Rights et al., "Coalition Comment to OMB on Privacy Impact Assessments," April 1, 2024, https://civilrights.org/resource/coalition-comment-to-omb-on-privacy-impact-assessments/.

[91] See EPIC, "Comment to OMB"; see also Faiza Patel and Patrick C. Toomey, "Bringing Transparency to National Security Uses of Artificial Intelligence," *Just Security*, April 4, 2024, https://www.justsecurity.org/94113/bringing-transparency-to-national-security-uses-of-artificial-intelligence.

[92] For a more thorough discussion on the current PIA compliance failures, the important role PIAs play in transparency and mitigating privacy risks, and the improvements needed to make PIAs more effective, see EPIC, "Comment to OMB."

agencies. These secrecy provisions have historically frustrated transparency and oversight efforts eroding accountability.[93]

In addition, **agencies that acquire CAI, or that contract for services that rely on third-party use of CAI, should be required to document and report their handling of that information**. Documentation should include the purpose of acquisition, how the agency intends to use the data, and the nature, source, and volume of the data; any licensing agreements or contract restrictions applicable to that information; the authority under which the information was acquired, used, created, or disseminated; any safeguards applied to the information, such as access protocols or use restrictions; and who participated in the procurement and approval process. When agencies contract with vendors, they should ensure that those private entities fully disclose the information necessary to comply with this requirement. Agencies should be **required to submit this documentation annually to Congress, with a classified annex if necessary.** Each agency should also be r**equired to make the report available to the public (with any classified information redacted) in a machine-readable, open format and without restrictions on use.**

C. [Q1, 9, 14] Refine Data Policies and Applicable Legal Frameworks for AI Systems Specifically

Given the central role of data in many AI systems, including potentially CAI for training AI technologies or as input to be processed, we also offer recommendations specific to OMB's policies on AI systems. OMB should adopt refinements in its AI guidance to impose rigor on agencies' reporting regarding AI use cases that involve CAI. For instance, OMB should **direct agencies to disclose sufficient details about the AI use cases in their inventories, such as a covered AI system's inputs and outputs, for the public to discern the role of CAI, if any, and understand the potential implications for their privacy and legal rights**. These and other improvements[94] would go a long way toward promoting responsible use of CAI by federal agencies and enabling public oversight and accountability.

V. Conclusion

The undersigned organizations welcome OMB's interest in advancing responsible handling of CAI by federal agencies. OMB guidelines that incorporate the above recommendations will help agencies align their handling of CAI with constitutional and legal restrictions that protect privacy, security, and civil liberties. For any questions, please contact Emile Ayoub (Brennan Center for Justice) at ayoube@brennan.law.nyu.edu, Kate Oh (Demand Progress Education Fund) at kate@demandprogress.org, Jason Taper (S.T.O.P.) at jason@stopspying.org, and Jeramie Scott (EPIC) at jscott@epic.org.

---

[93] See, e.g., Carey Shenkman et al., *Legal Loopholes and Data for Dollars*.

[94] See Center for Democracy & Technology et al., "Priorities for Office of Management & Budget Memorandum on Advancing Governance, Innovation, and Risk Management for Agency Use of AI," January 2024, https://cdt.org/wp-content/uploads/2024/01/Priorities-for-Office-of-Management-and-Budget-Memorandum-on-Agency-Use-of-AI.pdf.

Respectfully submitted,

Brennan Center for Justice
Demand Progress Education Fund
Electronic Privacy Information Center
Surveillance Technology Oversight Project
Advocacy for Principled Action in Government
Center for Democracy and Technology
Due Process Institute
Electronic Frontier Foundation
Free Press
Government Information Watch
New America's Open Technology Institute
Organization for Identity & Cultural Development
Privacy Rights Clearinghouse
Project for Privacy and Surveillance Accountability
Restore The Fourth
Secure Justice