STUDENT NOTES

Law Enforcement's Use of Commercially Acquired Information: How Can Congress Strike a Legislative Balance Between Privacy Concerns and National Security Risks in the Absence of Fourth Amendment Protections?

Susannah Gilmore*

I. INTRODUCTION

Immediately after 9/11, droves of data companies, financial institutions, service providers, carriers, and search engines opened their records to help law enforcement locate suspected terrorists.[1] One company in particular—called Matrix— successfully identified a hijacker and several of the FBI's top suspects using only a commercial database.[2] Impressed by its results, the government set aside $8 million to use Matrix to assist state and local law enforcement investigations.[3] A year later, the same technology helped catch the D.C. sniper.[4] But by 2005, public concern about privacy caused the government to withdraw its funding, and the technology was instead sold to LexisNexis for over $700 million.[5] A new market for data collection, analysis, and brokerage swiftly emerged. Today, the government is one of LexisNexis's biggest customers, routinely purchasing commercial data to aid its investigations and law enforcement efforts.[6]

The modern data brokerage market offers a virtually unlimited supply of personal data that private buyers and the government can legally purchase and use. In the past few years, investigations revealed that federal agencies frequently use Commercially-Available Information ("CAI") for law enforcement and counterintelligence purposes—and they affirmatively assert that no warrant is necessary to

* Susannah Gilmore is a 2025 graduate of the University of Maryland Francis King Carey School of Law's evening law program. During law school, she worked full-time at the U.S. General Services Administration and the National Security Division of the Department of Justice. Susannah also holds a Bachelor of Arts in Political Science from the University of Virginia. I am endlessly grateful to my village of mentors, friends, colleagues and family who supported me in my studies during a turbulent year.

1. ROBERT O'HARROW, NO PLACE TO HIDE 6–7 (2005).
2. Michael Shnayerson, *The Net's Master Data-Miner*, VANITY FAIR (Dec. 2004), https://perma.cc/4A57-MWK5.
3. Robert O'Harrow, *Anti-Terror Database Got Show at White House*, WASH. POST. (May 21, 2004).
4. Matthew Hector, *Do We Really Have No Place to Hide?*, 24 J. Comp. & Info. L. 58, 65 (2005).
5. Robert O'Harrow, *LexisNexis to Buy Seisint for $775 Million*, WASH. POST. (July 14, 2004).
6. *See infra* Section II.b.

purchase this data.[7] This practice raises Fourth Amendment questions—can the government legally purchase sensitive and personal data on U.S. individuals without violating the Constitution? This Article argues that the answer is unfortunately "yes," because government purchases of commercial data do not constitute state action and individuals cannot have a reasonable expectation of privacy in data being offered on the open market. Since the Fourth Amendment does not prevent the government from purchasing CAI, legislative action is needed to reduce the amount of U.S. personal data being sold by data brokers and ensure responsible government use of CAI.

While ample legal scholarship criticizes law enforcement's use of CAI from a privacy perspective, there is little discussion of policy arguments in support of law enforcement's use of CAI, or in opposition to a blanket prohibition on government purchases of CAI.[8] This Article compares policy arguments supporting and opposing law enforcement's use of CAI, ultimately concluding that the current national security risks associated with prohibiting law enforcement from purchasing CAI outweigh individual privacy concerns. This Article also attempts to draw attention to the negative consequences that a premature restriction of law enforcement's use of CAI would have in the field of counterterrorism.[9]

That being said, there is still opportunity for Congress to strengthen privacy safeguards and ensure that law enforcement is using CAI safely and responsibly. There is also a severe need for legislation and regulation of data brokerage generally to prevent sensitive data on U.S. individuals being sold to foreign adversaries on the open market. This presents a serious national security risk that Congress should address before it overly restricts law enforcement's ability to purchase CAI. Otherwise, the United States would be at a global disadvantage in terms of access to data. This Article concludes by suggesting ideas for future legislation to address both the privacy and national-security risks associated with CAI while ensuring that the United States can still maintain effective counterterrorism programs.[10]

II. BACKGROUND

Data brokerage originally began by offering software and services to extract information from public records for background checks.[11] Today, data brokerage

7. *See infra* Section II.b.

8. A search of legal scholarship from the past four years found only one article criticizing legislative efforts to prohibit law enforcement from using CAI. *See* Aaron X. Sobel, *End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem*, 42 YALE L. & POL'Y REV. 176, 176-77 (2023). In contrast, there are at least four articles that argue in support of restricting or entirely prohibiting the law enforcement from using CAI. *See, e.g.*, Dori H. Rahbar, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades the Fourth Amendment* 122 COLUM. L. REV. 713 (2022); Rhea Bhatia, *A Loophole in the Fourth Amendment: The Government's Unregulated Purchase of Intimate Health Data*, 98 WASH. L. REV. ONLINE 67 (2024); Matthew Tokson, *Government Purchases of Private Data*, 59 WAKE FOREST L. REV. 270 (2024); Andrew Wade, *The Clocks Are Striking Thirteen: Congress, Not Courts, Must Save Us from Government Surveillance via Data Brokers*, 102 TEX. L. REV. 1099 (2024).

9. *See infra* Section IV.b.

10. *See infra* Part V.

11. GINA MARIE STEVENS, CONG. RSCH. SERV., DATA BROKERS: BACKGROUND AND INDUSTRY OVERVIEW 2–3 (May 3, 2007).

is a global market worth over $250 billion and is projected to nearly double in the next decade.[12] Modern data brokers collect and store individuals' personal information and then catalog, advertise and sell that information in bulk quantities on an open market.[13] In order to fully explore the current debate around law enforcement's use of CAI, it is necessary to first understand how the data brokerage industry became the massive market it is today, the types of data that brokers currently offer, and how law enforcement's use of CAI initially gained media attention and became a public discussion. This section begins first by briefly discussing the broader background of data brokerage markets, then exploring the recent history of law enforcement's use of CAI.[14]

A. History of Data Brokerage Markets

The data brokerage market gained traction in the early 2000s with the expansion of the internet and the invention of software programs with the capability to search multiple public databases for personal information.[15] Companies like ChoicePoint and LexisNexis used their technology to scour vast databases of public records to sell information to entities like insurance companies, employers, and law enforcement.[16] Over the past two decades, this practice has shifted to companies now acquiring data through more passive means, such as smartphone app data collection, software development kits, online cookies, and credit card companies, often without the user's knowledge or permission.[17] Many modern data brokers headquartered in the United States openly advertise bulk data on U.S. individuals that is valuable to law enforcement, such as geolocation points, internet metadata, demographics, and military service.[18]

In 2012, the Federal Trade Commission ("FTC") began studying how data brokers use personal information, citing an alarming lack of regulation and oversight for personal data flows.[19] These transactions are still largely unregulated in

12. *Data Broker Market: Global Industry Analysis and Forecast (2025-2032) by Data Category, Data Type, End- User and Region*, MAXIMIZE MARKET RESEARCH (Jan. 2025), https://perma.cc/3Z99-3ZP6 (attributing projected growth to a rising demand for data analytics of social media, online shopping, and consumer behavior, as well as artificial intelligence and machine learning technologies).

13. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i (2014).

14. *See infra* Sections II.a & II.b.

15. Stevens, *supra* note 11, at 2.

16. *Id.* at 3–4.

17. *See* Urbano Reviglio, *The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview*, 11 INTERNET POL'Y REV. 1, 5–6 (Aug. 4, 2022) (describing the variety of ways that data brokers collect information and how "information fatigue" can cause users to agree to collection without understanding its scope).

18. JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS 1 (2021). Major U.S-based data brokers offering these types of data packages include Acxiom, LexisNexis, Nielsen, Equifax, CoreLogic, Verisk, Oracle, and Epsilon. *Id.* at 3.

19. *FTC to Study Data Broker Industry's Collection and Use of Consumer Data*, FED. TRADE COMM'N (Dec. 18, 2012), https://perma.cc/DU8E-KP9Z ("There are no current laws requiring data brokers to maintain the privacy of consumer data unless they use that data for credit, employment, insurance, housing, or other similar purpose.").

the United States today, although some regulatory frameworks exist at the state level and in Europe.[20] This lack of regulation, combined with general public confusion about how data brokerage works, allows these companies to function unrestrained and with relatively little consumer opposition.[21]

B. Law Enforcement's Use of CAI

The federal government has used commercially available data for decades, often for criminal investigations, identity verification, and fraud detection.[22] For example, a 2006 Government Accountability Office ("GAO") report highlighted that the Department of Homeland Security had a $2.3 million contract with LexisNexis and other data brokers to conduct commercial queries on individuals and entities to support intelligence-gathering and prosecution efforts.[23] This report also listed the Federal Bureau of Investigation ("FBI") as the largest government consumer of commercially acquired data, with approximately $11 million worth of contracts with data brokers to support its intelligence and investigation efforts in Fiscal Year 2005.[24] Soon after, Congress amended the Foreign Intelligence Surveillance Act ("FISA") to add Section 702, which gave the government authority to compel telecommunications companies to assist in the collection of foreign intelligence by providing communications data directly to them.[25] Later amendments and reauthorizations to Section 702 established enhanced safeguards for privacy, but did not restrict law enforcement's ability to acquire intelligence commercially.[26]

Despite this history, law enforcement's use of CAI did not gain significant public attention until recently. Sparked by the 2013 intelligence leak by Edward Snowden and resulting public discourse over privacy concerns and government surveillance, a series of investigative reports and government memos revealed the role of CAI in law enforcement efforts.[27] Furthermore, the Supreme Court's landmark ruling in *Carpenter v. United States*,[28] holding that the Fourth Amendment prohibits warrantless government seizure of location data from

20. *Id.* at 2; *see infra* Section V.B.

21. Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://perma.cc/GE7X-M9GT (reporting that sixty-seven percent of Americans understand "little to nothing" about how private companies use their personal data, and this number has risen over the years).

22. U.S. GOV'T ACCOUNTABILITY OFF., GAO-06-421, AGENCY AND RESELLER ADHERENCE TO KEY PRIVACY PRINCIPLES 1 (2006).

23. *Id.* at 29.

24. *Id.* at 21–22. This report also noted that federal agencies were inconsistent in their approaches to protect individual privacy and their policies often did not incorporate internationally-accepted principles of Fair Information Practices. *Id.* at 50.

25. JOSHUA T. LOBERT, CONG. RSCH. SERV., IF11451, FOREIGN INTELLIGENCE SURVEILLANCE (FISA): AN OVERVIEW (2010).

26. FISA Amendments Reauthorization Act of 2017 Pub. L. No. 115-118, 132 Stat. 3; Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, 138 Stat. 862.

27. *See generally The state of privacy in post-Snowden America*, PEW RSCH. CTR. (Sept. 21, 2016), https://perma.cc/367U-Z638 (discussing generally the impact of Edward Snowden's intelligence leak on public opinions of privacy).

28. Carpenter v. United States, 585 U.S. 296 (2018).

phone companies,[29] prompted members of Congress to further explore the issue.

In January 2021, an unclassified memo from the Defense Intelligence Agency ("DIA") confirmed that the agency funds purchases of commercially acquired intelligence from private data brokers.[30] DIA expressed its opinion that *Carpenter* did not apply to CAI being used for intelligence purposes and that its actions were constitutional.[31] Because the Court did not address government collections for foreign intelligence purposes specifically, DIA argued that the decision was "narrow" and DIA's actions were instead governed by the Department of Defense's internal data handling manual.[32] DIA also stated that its data brokerage service does not filter domestic geolocation data points from foreign ones, and DIA instead removes domestic data points itself into a "separate database" that requires special approval for DIA personnel to query for data within it.[33]

A year later, the Office of the Director of National Intelligence ("ODNI") published a report recommending that the Intelligence Community restrict its use of commercially acquired intelligence.[34] This report acknowledged that CAI is extremely valuable to counterterrorism and counterintelligence efforts because it can be combined with traditional surveillance systems like SIGINT to expand its capabilities.[35] Further, the report argued that because CAI is available to other nations and foreign adversaries, the United States would be at a severe disadvantage if it were unable to have similar access.[36] Given this, ODNI recommended that the Intelligence Community develop privacy standards to ensure that purchases of CAI are precisely tailored to law enforcement's needs with stringent approval requirements corresponding to the level of sensitivity of the information acquired.[37] The report suggested the use of anonymization, filtering, and traditional minimization techniques to limit the amount of U.S. personal data collected and accessed.[38]

Awareness of federal law enforcement and intelligence agencies' use of CAI has increased in the past few years with news outlets reporting on these common practices at the Department of Homeland Security,[39] the Internal Revenue

29. *Id.* at 320–21.

30. CLARIFICATION OF INFORMATION BRIEFED DURING DIA'S 1 DECEMBER BRIEFING ON CTD, DEFENSE INTEL. AGENCY 1 (2021) ("DIA currently provides funding to another agency that purchases commercially available geolocation metadata aggregated from smartphones.").

31. *Id.* at 2.

32. *Id.*

33. *Id.* at 1.

34. OFF. OF THE DIR. OF NAT'L INTEL., SENIOR ADVISORY GRP., REPORT TO THE DIRECTOR OF NATIONAL INTELLIGENCE 2 (2022), https://perma.cc/RX3N-GKUA.

35. *Id.* at 9.

36. *Id.*

37. *Id.* at 27–28.

38. *Id.* at 28.

39. Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphones Data to Track People*, BUZZFEED NEWS (Oct. 30, 2020), https://perma.cc/G4R2-RJSG (reporting that the Department of Homeland Security frequently purchases cellphone geolocation data to assist in illegal border crossing investigations).

Service,[40] and the military.[41] While agencies use much of the information collected to investigate foreigners abroad, they often inadvertently sweep up a considerable amount of information on U.S. individuals.[42] Authorities like FISA and Section 702 help prevent misuse of these incidental collections, but no comprehensive legislation restricts how agencies can purchase and use CAI.[43] While legal challenges to the act of *selling* sensitive personal data (such as geolocation data) have been successful, there is little caselaw addressing the legality of law enforcement and the Intelligence Community's acquisition of such data.[44]

III. USE OF CAI BY LAW ENFORCEMENT IS NOT PROHIBITED BY THE FOURTH AMENDMENT

Many critics of law enforcement's use of CAI characterize the practice as a "loophole" to the Fourth Amendment because it allows the government to warrantlessly obtain personal information on the open market.[45] This criticism assumes that U.S. individuals have a reasonable expectation of privacy in their CAI being sold on the open market. But rather than a "loophole" in the Fourth Amendment being exploited by law enforcement, CAI operates in a legitimate, legal open market and is thus entirely out of the Fourth Amendment's scope for a number of reasons discussed in this section. This section begins first by establishing why U.S. individuals do not have a reasonable expectation of privacy in CAI being purchased by the government.[46] Then, this Section turns to method-based arguments that support the legality of law enforcement's use of CAI.[47]

A. Individuals Do Not Have a Reasonable Expectation of Privacy in Commercial Intelligence at the Moment the Government Acquires It

The Fourth Amendment protects U.S. persons from unreasonable government searches and seizures.[48] For such a search to occur, an individual must have a reasonable expectation of privacy in the object of the search, and this expectation

40. Letter from J. Russell George, Inspector Gen., Internal Rev. Serv., to Hon. Ron Wyden & Elizabeth Warren (Sept. 30, 2020), https://perma.cc/Z9QP-UAGA (notifying the senators that the Internal Revenue Service will investigate its Criminal Investigations unit's use of CAI and conduct a legal analysis on the practice).

41. Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), https://perma.cc/AQ5C-LLLW (detailing how a military counterterrorism branch bought location app data derived from smartphone apps for assistance in its overseas operations).

42. Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, NY TIMES (Jan. 25, 2021), https://perma.cc/X55A-9Q23.

43. *Minimizing United States Person Information Under FISA Section 702*, INTEL.GOV.

44. *See, e.g.*, X-Mode Soc., Inc., 2024 FTC LEXIS 31, 21–23 (2024) (finding that a U.S. company's selling of geolocation points derived from smartphone data to the U.S. military without affirmative, express user consent was unlawful).

45. *See, e.g.*, Noah Chauvin, *New Legislation Would Close a Fourth Amendment Loophole*, BRENNAN CTR. (July 6, 2023), https://perma.cc/CW9N-JEPS.

46. *See infra* Section III.A.

47. *See infra* Section III.B.

48. U.S. CONST. amend. IV.

must be both subjective and objectively recognized by society.[49] Historically, courts held that individuals cannot have a legitimate expectation of privacy in any information that they voluntarily provide to third parties, such as telecommunications providers, mail services, and financial institutions—a principle known as the third-party doctrine.[50] This allowed the government to legally obtain information like call logs and eventually cellular site location information ("CSLI") from third party service providers without a warrant and use this information to prove a crime.

In 2018, the Supreme Court in *Carpenter* narrowed the third-party doctrine by holding that warrantless government access to historical CSLI records spanning a period of time of six days or more violates the Fourth Amendment.[51] In its opinion, the Court stressed privacy concerns stemming from the "encyclopedic" archive that CSLI could reveal about a person, claiming that a reasonable person would likely not expect their location data to be shared with the government by their cellular provider.[52] However, the Court also cautioned that its decision in *Carpenter* was a narrow one, and specifically noted that it did not address collection methods that involve "foreign affairs or national security."[53]

Given the narrow scope of *Carpenter*, it is important to initially establish that much, if not most, of the CAI obtained by law enforcement falls under the third-party doctrine because it is not CSLI. Law enforcement agencies buy a large variety of commercial data on the open market—such as social media data, browsing history, metadata, topographical maps—and these do not constitute a Fourth Amendment search under *United States v. Miller*.[54] For the instances where the government is actually purchasing CSLI exceeding the durational limit, a special needs warrant exception for national security and foreign intelligence almost certainly exists, as was alluded to in *Carpenter*.[55]

Even if this data collection was not a "special needs" or third-party doctrine exception, it likely evades Fourth Amendment purview because a lawful purchase does not constitute a "search." This principle is long-established and has not been challenged in recent Fourth Amendment jurisprudence like *Carpenter*. The Court in *United States v. Jacobsen*[56] offered a temporal limitation to Fourth Amendment searches, holding that an individual's reasonable expectation of privacy must be determined at the time the alleged "search" is actually conducted.[57] Thus, "[t]he reasonableness of an official invasion of the citizen's privacy must be appraised on the basis of the facts as they existed *at the time* that invasion

49. Katz v. United States, 389 U.S. 347, 361 (1967).
50. United States v. Miller, 425 U.S. 435, 443 (1976); Smith v. Maryland, 442 U.S. 735, 744 (1979).
51. Carpenter v. United States, 585 U.S. 296, 322–23 (2018).
52. *Id.* at 309-10.′
53. *Id.* at 316.
54. OFF. OF THE DIR. OF NAT'L INTEL, *supra* note 35, at 8–11, 19.
55. *Id.* at 19–20;
56. United States v. Jacobsen, 466 U.S. 109 (1983).
57. *Id.* at 115. This principle was also upheld in United States v. Smith, 210 F. Supp. 2d 1096, 1102–03 (D. Neb., 2001).

occurred."[58] In *Jacobsen*, the Court applied this reasoning to a government agency inspecting the contents of a mailed package that had been already opened by freight carrier employees, finding that the employees' initial search of the package destroyed a reasonable expectation of privacy before law enforcement even arrived.[59]

The same reasoning can be directly applied to government purchases of CAI. Because an individual's privacy interests are already frustrated by the time their personal information is offered up for sale on the open market, subsequent government purchase of that information does not violate the Fourth Amendment. To fall under Fourth Amendment jurisdiction, one would have to prove valid state action.[60] Essentially, the government purchase would have to further extend from the data broker's "private search" or otherwise somehow coerce or compel the data broker to give the data to the government, thereby making the data broker a state actor.[61]

A mosaic-theory for a reasonable expectation of privacy offers the strongest argument for Fourth Amendment coverage, as one could theoretically argue that government's manipulation of CAI and combination with other datasets dramatically expands the amount and degree of personal information revealed about a particular person.[62] However, mosaic theories of privacy present a multitude of issues at the practical level, making it unlikely for a court to use them as a basis for Fourth Amendment applicability. For example, courts would face the difficult problem of defining precisely when a series of otherwise lawful government actions become a search—would this occur when the government combines CAI with any other existing database it has access to, or when the government executes a specific query within a CAI database?[63] These are difficult parameters to define and are better addressed by congressional or regulatory solutions than case law.

B. Method-Based Evaluations of Fourth Amendment Searches Support the Legality of Warrantless Acquisition of Commercial Intelligence

Other Supreme Court standards tailored to technology searches focus on whether the tool or technique used by law enforcement to gain information is one that is available to the general public. Searches using thermal imaging cameras or scent canines, for example, are deemed to violate an individual's reasonable expectation of privacy because they are conducted using technology and methods that were not available to the general public at the time of the search.[64] While

58. *Jacobsen*, 466 U.S. at 115. (emphasis added).

59. *Id.* at 126 (". . .the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct.").

60. Sobel, *supra* note 8, at 189–90.

61. *Id.*

62. OFF. OF THE DIR. OF NAT'L INTEL, *supra* note 35.

63. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 346–47 (2012), https://perma.cc/2QAH-K9XF.

64. Kyllo v. United States, 533 U.S. 27, 40 (2001); Florida v. Jardines, 569 U.S. 1, 11–12 (2013).

these cases involved technology used to conduct a search, the same reasoning can be applied to commercial purchases. This characterization is supported by existing regulation: the Federal Acquisition Regulations defines a commercial item as being "of the type customarily used by the general public" and has been actually "sold" or "offered for sale" to the general public.[65]

With CAI, the general public has the ability to—and often does in fact—purchase vast quantities of commercial data and intelligence.[66] For example, a report in 2023 highlighted how a group of university researchers were able to privately purchase thousands of data points on military personnel that included information on health, finances, religious practices, phone numbers, and residential addresses for as little as $0.125 per military service member.[67] As recent legal scholarship notes, "[a]n agency buyer of data is definitionally a mere market participant," and this makes it extremely unlikely for a court to find the required state action that would trigger the Fourth Amendment.[68]

This could change in the future if the government's use of CAI becomes its predominant method to acquire intelligence and data brokerage starts to fulfil a "public function." But as discussed in the next section of this Article, the government appears to use CAI as a *supplement* to its traditional intelligence acquisition methods and also as a tool to ensure compliance with existing authorities like FISA.[69] Ultimately, as it currently stands, government use of CAI is entirely legal and unprotected by the Fourth Amendment. While proposed legislative solutions call attention to important privacy concerns, they undervalue the necessity of CAI in counterintelligence efforts, an issue to which this Article now turns.

IV. ANALYSIS

Critics on both sides of the argument have valid concerns and justifications for why law enforcement's warrantless use of CAI should or should not be allowed. On one hand, privacy advocates argue that using CAI allows the government to circumvent important minimization safeguards and also promotes a harmful global data brokerage market. Furthermore, because of a lack of regulation, the data obtained from private brokers is of questionable quality—an especially concerning fact when considering that this data may be used to justify deprivation of

65. FAR 2.101 (2024); *see also* Mike Petridis, *In General Public Use: An Unnecessary Test to Determine Whether the Use of Advanced Sensing Technology Was a Fourth Amendment Search*, TOURO L. REV. (Apr. 21, 2020), https://perma.cc/VL37-9G2L (arguing that courts should use the property-based factors provided in the Federal Acquisition Regulation to determine whether a search method is available to the general public).

66. In addition to law enforcement, data broker customers include advertisers, political campaigns, financial institutions, landlords, employers, other data brokers, and internet "doxxers." Nica Latto, *Data Brokers: Everything You Need to Know*, AVAST (Jan. 3, 2024), https://perma.cc/H2UK-XQ5K.

67. JUSTIN SHERMAN, HAYLEY BARTON, ADEN KLEIN, BRADY KRUSE, AND ANUSHKA SRINIVASAN, DATA BROKERS AND THE SALE OF DATA ON U.S. MILITARY PERSONNEL: RISKS TO PRIVACY, SAFETY AND NATIONAL SECURITY 5 (2023).

68. Sobel, *supra* note 8, at 193.

69. OFF. OF THE DIR. OF NAT'L INTEL, *supra* note 35, at 10, 14; *see supra* Section IV.B.

one's fundamental liberties.[70] On the other hand, there are compelling national-security arguments that government access to CAI is crucial to counterintelligence efforts, and prohibiting the government from accessing CAI would only give U.S. adversaries an advantage.[71] This section explores in-depth these policy arguments for and against government use of CAI, concluding that ultimately, the risks of prematurely prohibiting law enforcement use of CAI outweigh the privacy concerns raised.[72]

A. Policy Arguments Against Government Use of CAI

The public debate around law enforcement's use of CAI draws attention to important privacy issues. First, the government's ability to buy sensitive data, like geolocation points for example, eliminates at least some need to go through traditional authorities, namely FISA. And FISA includes important safeguards to protect privacy that are not present with CAI, like minimization requirements, querying restrictions, and judicial review of non-compliance through the FISA Court.[73] While FISA has historically been the primary intelligence collection method since its enactment over forty years ago, the vast quantities and variety of types of commercial data available on the open market (which expand every year) may eventually make it wholly unnecessary for agencies to use FISA at all.[74] The lack of publicly available information on exactly how much law enforcement and intelligence agencies rely on CAI as opposed to FISA makes it difficult to estimate the extent of FISA "circumvention," but the privacy concerns remain valid across demographic groups and political partisanships.[75] While trust in the government's ability to self-police this usage is lacking, there is overwhelming public support for regulation.[76]

Second, the government's participation in the data brokerage market itself is harmful because it promotes and perpetuates a harmful practice that violates personal privacy of U.S. individuals—including U.S. citizens, lawful residents, and those living within the United States. Beyond the issues associated with the government's use of CAI itself, data brokerage harms personal privacy and has concerning implications for civil rights. Data brokers collect vast amounts of data on personal browsing activities, purchases, voter registration, bankruptcy information, and other sensitive information, often without the subject's knowledge or

70. *See infra* Section IV.A.

71. *See infra* Seciton IV.B.

72. *See infra* Sections IV.A & IV.B.

73. Elizabeth Goitein, *How to Fix U.S. Surveillance Law*, BRENNAN CTR. (July 18, 2023), https://perma.cc/TTK9-MHK2.

74. *See supra* Section II.A (describing the types and quantities of commercial intelligence available on the open market).

75. McClain et al., *supra* note 21 (reporting that seventy-one percent of Americans are concerned about how the government uses their personal data).

76. *Id.* (reporting that seventy-two percent of Americans believe there should be more regulation of data brokers generally).

consent.[77] This information is collected and catalogued by data brokers and collectively covers almost every single American household.[78] This creates risk to U.S. individuals by allowing bad actors to gain significant insight into one's personal life, making it easier to harass, stalk, blackmail, defraud, or steal one's identity.[79] Because data brokers also collect data on race, ethnicity, marital status, gender, and immigration status, there are potential civil rights issues as well. Companies could use this data to discriminate against certain individuals, or discriminately target advertising to specific groups.[80] When this practice is compounded by artificial intelligence-driven algorithms to determine costs, prices for goods and services could be set unfairly high for minority groups.[81]

Third, personal data obtained from data brokers can be inaccurate or misleading. Data brokers often compile data from multiple sources, including other data brokers,[82] and multiple reports note significant inaccuracies in consumer profiles,[83] geolocation data,[84] and biographical information.[85] Compared to traditional intelligence gathering under FISA where law enforcement agencies receive data directly from the companies that originally obtain it, commercial data is less reliable. Data brokers simply do not have the same incentive to ensure their data is 100% accurate because perfect accuracy is not necessary to meet most private clients' marketing goals.[86] Because CAI has the potential to invade privacy and justify deprivation of one's fundamental liberties, law enforcement should adhere to a higher set of quality and accuracy standards that private data brokerage cannot yet deliver. The recent emergence of artificial intelligence tools heightens this risk of unreliability even more by allowing larger inferences to be drawn about individuals.[87]

---

77. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 48 (2014).

78. *Id.* at 46.

79. *Id.* at 48.

80. Sherman, *supra* note 18, at 8–9.

81. *Id.* at 9.

82. Rahbar, *supra* note 8, at 736.

83. Nico Neumann, Catherine E. Tucker, and Timothy Whitfeld, *How Effective Is Third-Party Consumer Profiling and Audience Delivery? Evidence from Field Studies*, 38 MARKETING SCI. 913 (2019) (finding that "Audience segments vary greatly in quality and are often inaccurate across leading data brokers.").

84. MOBILE MARKETING ASS'N, DEMYSTIFYING LOCATION DATA ACCURACY 11 (2015).

85. LEVI KAPLAN, ALAN MISLOVE & PIOTR SAPIEZYŃZKI, MEASURING BIASES IN A DATA BROKER'S COVERAGE (2017), https://perma.cc/BT8D-GPJ4.

86. HENRIK TWETMAN & GUNDARS BERGMANIS-KORATS, DATA BROKERS AND SECURITY: RISKS AND VULNERABILITIES RELATED TO COMMERCIALLY AVAILABLE DATA 14 (2020); *see generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 41 (2014) (noting that data brokers advertise the "utility and predictive quality" of their data, often taking no responsibility for the data's accuracy).

87. *See* Notice of Request for Information, 89 Fed. Reg. 83517-18 (2024). This notice recognizes that the use of artificial intelligence in combination with data brokerage may increase privacy risks by facilitating collection of personal data in terms of speed and quantity and allowing data brokers to make AI-driven inferences on individuals.

B. Policy Arguments in Support of Government Use of CAI

Despite its controversy, law enforcement's use of CAI is an important tool to mitigate national security risks and run effective counterterrorism programs.[88] When combined with traditional intelligence acquired under FISA, CAI can dramatically expand law enforcement's ability to detect and find criminals in a short amount of time.[89]

CAI also helps law enforcement ensure compliance with existing FISA minimization procedures because it can be used to filter out information associated with U.S. persons within a large database.[90] In 2022, ODNI reported that CAI is similarly useful to determine whether data acquired under SIGINT or other collection programs is associated with non-U.S. persons.[91] ODNI has also noted that CAI is useful for clandestine human intelligence operations by allowing cover development and proper planning.[92]

By far the most compelling argument in support of law enforcement's use of CAI is that such use is currently necessary to ensure the success of U.S. counterintelligence efforts. Data brokers frequently advertise and sell the same personal data purchased by law enforcement to foreign adversaries and bad actors.[93] If the government was unable to have access to this same data, U.S. intelligence agencies would be at a severe disadvantage compared to the rest of the world, and this could have life-threatening consequences to critical counterintelligence efforts. As noted in a recent executive order, foreign adversaries can use sensitive personal data to "engage in espionage, influence, kinetic, or cyber operations or to identify other personal strategic advantages over the United States," create and refine AI tools, build profiles on the U.S. military, and exploit foreign policy threats.[94] The sale of geolocation data to foreign adversaries is especially concerning because it can reveal the physical location of military service members or government employees, as well as the location of sensitive government facilities.[95] When layered with other datasets, this data allows buyers to uncover intimate details about a person's life—e.g., their religion, sexuality, health conditions, and finances.[96] Even when geolocation is sold as "encrypted" by data brokers, countries like China routinely harvest encrypted data with the intention of decrypting and re-identifying it with future quantum

88. *Americans Support Law Enforcement's Use of Data Fusion Tools to Help Solve Crimes Faster*, TRANSUNION (Oct. 17, 2016), https://perma.cc/4UQ3-AYJG (reporting that eighty-one percent of Americans believe law enforcement is obligated to use publicly available information to solve crimes).

89. *Id.*

90. OFF. OF THE DIR. OF NAT'L INTEL, *supra* note 35, at 10, 14

91. *Id.* at 10.

92. *Id.*

93. *Id.* at 11 (noting that CAI "offers intelligence benefits to our adversaries, some of which may create counter-intelligence risk for the IC.").

94. Exec. Order No. 14117, 89 Fed. Reg. 15421, 15421 (Feb. 28, 2024).

95. Justin Sherman, *Data Brokers and Threats to Government Employees*, LAWFARE (Oct. 22, 2024), https://perma.cc/JJA6-35N5.

96. *Id.*

technology capability.[97] There are also significant risks associated with the sale of genomic data. A 2021 report from the National Counterintelligence and Security Center revealed that China strategically amasses large quantities of healthcare and genomic data from genetic testing companies and clinical trials.[98] This practice means that China has the ability to "precisely target individuals in foreign governments . . . for potential surveillance, manipulation or extortion."[99] Given the critical national security risk presented by allowing U.S. companies and data brokers to sell this data, there must be targeted legislation and regulation to limit parties from obtaining or selling sensitive data in the first place.

While current legislative efforts have focused on restricting U.S. law enforcement from using CAI, this solution does not solve the larger underlying problem: that data brokers have amassed concerningly large amounts of sensitive and personal data on U.S. individuals, which they then sell on the open market to any buyer willing to pay. Preventing U.S. law enforcement from accessing these databases is a premature solution that would only disadvantage the United States while other countries are meanwhile able to freely purchase this data on the open market.[100] This kind of legislation metaphorically puts the cart before the horse, and other legislative and regulatory efforts are first needed to limit data brokerage generally and prevent U.S. personal data from falling into the wrong hands.

V. OPTIONS FOR REFORM

Effective legislation is needed to limit the amount of personal data on U.S. individuals being sold by data brokers before curtailing law enforcement's access to this data. Some legislation and regulatory efforts have begun to do this, but a more comprehensive statutory scheme would be more effective to restrict data brokers generally. To put it simply, data brokers benefit immensely from the lack of government regulation of their transactions and will continue to collect and sell personal data until restricted by law.[101]

A. Restricting Data Brokerage Generally

One approach to restrict the amount of personal data on U.S. individuals being sold by data brokers involves laws that condition a broker's ability to sell this data on the individual's consent. Models of these consent-based restrictions exist at both the state level and internationally. At the state level, California's Consumer Privacy

97. Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 89 Fed. Reg. 86116, 86127 (proposed Oct. 29, 2024).

98. NAT'L COUNTERINTEL. & SEC. CTR., CHINA'S COLLECTION OF GENOMIC AND OTHER HEALTHCARE DATA FROM AMERICA: RISKS TO PRIVACY AND U.S. ECONOMIC AND NATIONAL SECURITY 3–4 (Feb. 2021), https://perma.cc/AMM7-BUHV.

99. *Id.* at 4.

100. *See* Sobel, *supra* note 8, at 232–33 (explaining that current legislative proposals focus too specifically on a "downstream effect" and that Congress should instead address the source problem of "invasive" data being transacted on the open market).

101. Reviglio, *supra* note 17, at 2.

Act[102] offers its residents the most privacy and control over how much of their personal data can be sold by brokers. It requires companies to allow residents to opt out of having their personal data sold and also imposes due diligence responsibilities on companies to know what personal data they are collecting and to whom it is being sold or disclosed.[103] Similarly, the European General Data Protection ("GDPR") requires companies to obtain informed user consent before sharing their data, allow users the option to opt out of data sharing at any time, and comply with due diligence requirements to ensure proper safeguarding of personal data.[104] These types of efforts successfully incentivize companies to change their data retention policies and data security measures while also increasing consumer awareness about how their personal data is used.[105]

Other approaches to this problem could take aim at data brokers specifically and their transactions with foreign adversaries. Congress could incentivize responsible data brokerage by requiring data brokers to register in a public database managed by the Office of Management and Budget and could then subject brokers to public reporting requirements on the amount and types of personal data they sell. Congress could also require annual audits for data brokers to make sure they are complying with due diligence standards to protect privacy.[106]

The recently-passed Protecting Americans' Data from Foreign Adversaries Act of 2024 ("PADFAA") prohibits data brokers from selling personally identifiable sensitive data of U.S. persons to any foreign adversary or entity controlled by a foreign adversary.[107] PADFAA allows the FTC to bring civil enforcement actions against data brokers that violate the prohibition.[108] While this approach is a significant step forward, it only restricts U.S. data brokers themselves and leaves buyers off the hook. Comprehensive legislation should target U.S. companies that directly collect and sell this personal data in the first place, such as social media companies, telecommunication services, apps, and the healthcare sector and hold them accountable for knowingly selling data of U.S. persons to foreign adversaries. Along these lines, a recently promulgated rule from the Department of Justice prohibits certain transactions that would allow a foreign adversary or a person of concern to gain access to certain kinds of government related data or bulk U.S. sensitive personal data.[109]

---

102. Consumer Privacy Act, Assemb. B. 375, 2017–2018 Sess. (Cal. 2018).

103. *Id.*

104. Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EX.

105. Sari Richmond, *Effectiveness and Implications of the California Consumer Privacy Act*, NW. UNDERGRADUATE L.J. (Aug. 25, 2024), https://perma.cc/Q2GB-8LL4; Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 13, 2021), https://perma.cc/GA38-WVUN.

106. Bhatia, *supra* note 8, at 100.

107. Public Law 118–50, div. I 138 Stat. 895, 960 (2024).

108. *Id.*

109. Press Release, Justice Department Issues Final Rule Addressing Threat Posed by Foreign Adversaries' Access to Americans' Sensitive Data, DEP'T OF JUST. NAT'L SEC'Y DIV. (Dec. 27, 2024), https://perma.cc/W2KZ-MDW6.

Future legislation should incorporate a mix of tighter restrictions on data broker sales and accountability for corporate collectors of personal data. Additional due diligence requirements for companies could include stringent audit requirements, minimum cybersecurity restrictions, minimum logical and physical access control requirements, recordkeeping mandates and standards, and advanced encryption techniques.[110] Beyond this, Congress should give agencies like the FTC adequate discretionary authority to investigate suspect data brokerage firms that could pose privacy or exploitation risks.[111]

B. Ensuring Responsible Law Enforcement Use of CAI

Congress should also work to ensure responsible government use of CAI. While some agencies have voluntarily agreed to stop buying CAI or limit their use of it internally, there is a significant lack of information on exactly how much and what type of CAI government agencies purchase that future legislation could address.[112]

The first major statutory reform to target law enforcement's use of CAI came to light in April of 2024, when the House passed the Fourth Amendment Is Not For Sale Act.[113] This Act seeks to ban the government from purchasing CAI, sharing it with law enforcement and intelligence agencies, and using it in judicial proceedings without a warrant.[114] It also specifies that law enforcement and intelligence agencies should exclusively use FISA to conduct electronic surveillance.[115] While the bill was introduced as bipartisan, it had significant opposition.[116] Much of this opposition highlights how the Act would delay and restrict law enforcement investigations and the need to balance these concerns with reasonable privacy protections.[117]

President Biden also opposed the bill. During a brief statement from the White House in April of 2024, he expressed his concern about the bill unduly restricting law enforcement and hindering national security and counterterrorism efforts.[118] Instead, Biden urged privacy efforts to focus first on preventing foreign

110. *See, e.g.,* Notice of Available of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528 (Jan. 8, 2025) (establishing security requirements for certain transactions of American bulk sensitive personal data under a Department of Justice final rule).

111. Sherman, *supra* note 18, at 2.

112. In 2023, Customs and Border Protection announced that it would voluntarily stop buying smartphone geolocation data in response to a scathing report by its Office of the Inspector General. Joseph Cox, *Customs and Border Protection Says It Will Stop Buying Smartphone Location Data*, 404 (Sept. 12, 2023), https://perma.cc/H4NJ-C2ZV.

113. H.R. 4639, 118th Cong. (2024) (as passed by House, Apr. 17, 2024).

114. *Id.*

115. H.R. 4639, 118th Cong. (2024) (as passed by House, Apr. 17, 2024).

116. The bill was opposed by the House Intelligence Committee Chairman (Turner OH-R) and Ranking Minotiry Leader (Himes CT-D). CLERK, U.S. HOUSE OF REPS., Roll Call 136 on Passage of Bill Number: H.R. 4639, The Fourth Amendment Is Not For Sale Act (Apr. 17, 2024).

117. 170 CONG. REC. H2459–68 (Apr. 17. 2024) (statement of Rep. John Rutherford and Rep. Mark Turner).

118. EXEC. OFF. OF THE PRES., STATEMENT OF ADMINISTRATION POLICY: H.R. 4639 – FOURTH AMENDMENT IS NOT FOR SALE ACT (2024) (stating that the Biden Administration "strongly opposes" the bill).

adversaries and private parties from accessing CAI and second on establishing policy for the "reasonable collection" of CAI.[119]

Instead of imposing a blanket ban on law enforcement use of CAI through the Fourth Amendment Is Not for Sale Act, Congress should focus on ensuring that law enforcement agencies have proper policies and procedures in place to safeguard personal CAI pertaining to U.S. persons. Along these lines, ODNI has published guidelines that contain numerous recommendations for access controls, heightened supervision, and privacy-enhancing techniques to use when handling CAI and minimizing privacy intrusions.[120] A more recent framework published in May of 2024 includes recommendations that mirror those for FISA.[121] For example, ODNI recommends that the Attorney General establish procedures for conducting and auditing queries, which include a limit on the amount of employees that are allowed to run queries and setting standards to make query terms as narrow as possible.[122] The framework also contains limits on data retention and requirements for agencies to annually report to Congress on the amount and types of sensitive CAI accessed by law enforcement.[123] Effective legislative efforts could solidify these recommendations, which would still allow for responsible use of CAI by law enforcement while also enhancing privacy.

To prevent Fourth Amendment intrusions, Congress should take steps to ensure that government purchases of CAI do not become "state actions." As mentioned earlier in this Article, a Fourth Amendment issue could arise if CAI becomes the predominant method to acquire intelligence and data brokers start to fulfil a "public function" by providing the government with highly unique and customized datasets that are not necessarily available to the general public.[124] To prevent this, Congress could enact legislation to prohibit agencies from requesting customized CAI datasets, thus forcing agencies to only utilize "off the shelf" datasets that are also available to other non-government buyers.[125]

VI. CONCLUSION

The emergence of CAI as a law enforcement tool has sparked an important public discussion of how Fourth Amendment privacy protections should apply to purchases of highly personal and sensitive datasets on U.S. individuals. More broadly, this calls attention to the problematic industry of data brokerage and the

119. *Id.* (mentioning the goals within Biden's recent Executive Order 14117).

120. OFF. OF THE DIR. OF NAT'L INTEL, *supra* note 35.

121. OFF. OF THE DIR. OF NAT'L INTEL, FACTSHEET: INTELLIGENCE COMMUNITY POLICY FRAMEWORK FOR COMMERCIALLY AVAILABLE INFORMATION (May 2024).

122. *Id.*

123. *Id.* at 10.

124. *See supra* Section III.B. Some legal scholars argue that this practice is already occurring, which would raise Fourth Amendment implications. *See* Tokson, *supra* note 8, at 5–6, 26-28.

125. Steven Szymanski, *Is the Fourth Amendment Really for Sale? The Defense Intelligence Agency's Purchase of Commercially Available Data*, J. NAT'L SEC'Y L. & POL'Y (June 9, 2021), https://perma.cc/89HV-5KGS ("If Congress remains concerned about the DIA's process, it should use a precise scalpel rather than a sledgehammer-like fulsome ban.").

fact that U.S. law enforcement agencies are not the only customers purchasing this data—brokers routinely sell the same datasets to foreign adversaries who strategically collect this information to advance their own policy objectives.[126] Because the Fourth Amendment likely does not prevent the government from buying this data, legislative and regulatory reform is needed to ensure responsible government use of CAI with similar restrictions as those found in FISA, such as minimization requirements, restricted queries, and increased supervision.[127]

It is especially important however to ensure that Congress does not categorically prohibit law enforcement from using CAI, because doing so would disadvantage the United States in counterterrorism efforts and would do nothing to prevent foreign adversaries and bad actors from purchasing this data. A balanced approach would simultaneously focus on increased regulation and oversight of the data brokerage market generally, increased accountability for companies that collect personal data, and responsible use of CAI by law enforcement.[128]

126. *See supra* Section IV.C.
127. *See supra* Parts III & IV.
128. *See supra* Part V.

***