

Legal Loopholes and Data for Dollars

How Law Enforcement and
Intelligence Agencies Are Buying
Your Data from Brokers



The Center for Democracy & Technology (CDT) is a 25-year-old 501(c)(3) nonpartisan nonprofit organization working to promote democratic values by shaping technology policy and architecture. The organisation is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

References in this report include original links as well as links archived and shortened by the [Perma.cc](#) service. The Perma.cc links also contain information on the date of retrieval and archive.



This report is licensed under a Creative Commons Attribution-Sharealike 4.0 International License.



Legal Loopholes and Data for Dollars

How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers

Authors

Carey Shenkman*
Sharon Bradford Franklin
Greg Nojeim
Dhanaraj Thakur

* Independent consultant and Human Rights Attorney

WITH CONTRIBUTIONS BY

Samir Jain, Ari Goldberg, Tim Hoagland, and Will Adler.

ACKNOWLEDGEMENTS

We thank David Hoffman and Harlan Yu for their valuable feedback. We also thank the various experts from academia, the media, and civil society who spoke to us and who helped inform the analysis in this paper. All views in this report are those of CDT.

This work is made possible through a grant from the John S. and James L. Knight Foundation.

SUGGESTED CITATION


Shenkman, C., Franklin, S.B., Nojeim, G., and Thakur, D. (2021) Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers. Center for Democracy & Technology.

Contents

Introduction	5
Key Findings	7
I. The Data Broker Ecosystem	9
A. How brokers acquire data	10
B. Data supply chains	12
II. Legal Framework	15
A. The loophole in the Electronic Communications Privacy Act (ECPA)	15
B. The Supreme Court recognized the sensitivity of device location information in Carpenter	17
C. Legal considerations for intelligence agencies	18
D. Overbroad and misleading use of terms 'open source' and 'publicly available'	19
III. Federal Agency Use Cases for Brokered Data	22
A. Mobile device geolocation data	22
B. Communications data and metadata	29
C. License plate reader (LPR) data	30
D. Other types of brokered data	33
Recommendations	36
A. For Policymakers	37
B. For Private Companies	40
Annex - Methods, Challenges, and Tactics for Further Research	42
References	44

Introduction

Our research for this report involved interviewing experts on this issue and reviewing approximately 150 publicly available documents covering awards, solicitations, requests for proposals, and related information on contracts.



Typically, government agencies seeking access to the personal electronic data of Americans must comply with a legal process to obtain that data. That process can be mandated by the Constitution (the Fourth Amendment’s warrant and probable cause requirement) or by statute (such as the federal Electronic Communications Privacy Act, or various state laws). This report examines the concerning and rising practice of federal agencies sidestepping these legal requirements by obtaining data on Americans through commercial purchases from data brokers.

Our research for this report involved interviewing experts on this issue and reviewing approximately 150 publicly available documents covering awards, solicitations, requests for proposals, and related information on contracts. We found significant evidence of agencies exploiting loopholes in existing law by purchasing data from private data brokers. The practice has prompted scrutiny from government watchdogs as well as members of Congress ([Tau, 2021a](#); [Wyden, 2021](#)).

The problem is a byproduct of the lucrative private market for personal data, where many companies that offer online services collect, analyze, and sell data about individuals using those services. This data is aggregated by companies called ‘data brokers’ that typically lack any direct relationship with the individuals whose data they collect and sell, but may accumulate personal data from multiple sources with varying degrees of granularity, ranging from anonymized trends to the specific locations of individuals at specific times. Advertisers, retailers, and other companies may then seek access to data for varied commercial purposes.

As our research demonstrates, law enforcement and intelligence agencies are among the customers of some data brokers, spending millions of dollars to gain access to private sector databases which often contain very sensitive and very personal information on individuals.

One recent example of this pattern is the Department of Justice’s use of commercially aggregated data in prosecutions surrounding the Capitol Breach of 2021. The Justice Department indicated in a federal court filing that it had utilized “[l]ocation history data for thousands of devices present inside the Capitol (obtained from a variety of sources including Google and multiple data aggregation companies),” (*Grand Jury Action No. 21-20 (BAH)*, 2021). In another filing, the Justice Department indicated that data was obtained from “searches of ten data

aggregation companies,” (*United States v. Perretta*, 2021). The filings did not indicate who those aggregation companies were.

There is no clear limit on the potential availability of commercially acquired data that would typically require legal process to obtain. In the words of one presenter to law enforcement at a location-analytics conference, “cell phone data, social media feeds, license-plate reader and automatic-vehicle locator systems are readily available to investigators” ([Delaney & Beck, 2014](#)). Law enforcement and intelligence agencies could obtain these types of personal data from different sources, including publicly available information (e.g., public posts on the web), access to company records through legal process (e.g., a court order directing an internet service provider to turn over information), or data brokers. Of these various sources, we have very little insight into agencies’ engagement with data brokers.

This report seeks to shed light on the nature and scale of the data broker to federal law enforcement and intelligence pipeline, and how law enforcement and intelligence agencies are relying on such purchases in situations where they should be required to obtain a warrant or other formal legal process to compel disclosure of the data. The report concludes with a series of recommendations to address these findings. Most critically, Congress should act to close the loophole that is permitting government agencies to evade requirements that they obtain a warrant or other legal process by instead purchasing sensitive information from data brokers.



Key Findings

#1 : Multiple forms of sensitive data, including location, communications, biometric, and license plate reader data, are sold by data brokers to law enforcement and intelligence agencies, and the practice is increasing, with multiple agencies spending upwards of tens of millions of dollars on multi-year contracts.

#2: Government agencies seeking to purchase data frequently use terms like ‘open source’ and ‘publicly available’ in their purchase orders and contracts, suggesting that they are only seeking information such as public social media posts that people knowingly make available to the public. However, government purchase orders and contracts frequently use these terms to include information collected specifically for a given agency that is not actually available to the public or any other consumer. The broad and misleading usage of these terms undermines governmental claims that agencies are permitted to collect such information on the basis that it is generally out there in the public and individuals therefore lack a reasonable expectation of privacy in such sensitive data.

#3: Law enforcement and intelligence agencies often categorize procurement contracts through opaque or technical designations that obscure the nature of the data being purchased, the uses to which they will be put, and the privacy consequences.

#4: The Electronic Communications Privacy Act effectively contains a loophole allowing law enforcement to acquire communications data commercially from data brokers and evade otherwise applicable requirements that they must use legal process to obtain data directly from service providers. The Fourth Amendment Is Not for Sale Act would address this critical shortcoming and close this loophole, which was implemented three decades before data broker practices became widespread. Congress should act now to pass this legislation.

#5: In the 2018 landmark case *Carpenter v. United States*, the Supreme Court held that the government must obtain a warrant in order to collect cell site location information (CSLI) for seven days or more, recognizing that people have a “reasonable expectation of privacy” in certain digital information. The broad language of the opinion suggests


that the government must also obtain a warrant in order to access sensitive personal information in contexts beyond the facts of the case. Thus, when law enforcement and intelligence agencies purchase certain personal data about Americans from data brokers, they are evading Fourth Amendment safeguards as recognized by the Supreme Court. These agencies should comply with Fourth Amendment standards and cease purchasing sensitive data that reveal the “privacies of life” under the Supreme Court’s analysis in *Carpenter*.

#6: Privacy policies of data brokers are often broadly drafted and do not offer meaningful transparency or protection against direct or downstream sale of data to government agencies. Consumers are also typically unaware what brokers possess their data—and hence what policies even apply. Thus, in addition to regulations limiting the ability of law enforcement and intelligence agencies to purchase information from data brokers, federal law should regulate data broker collection and processing of information, and provide consumers with the ability to understand what information data brokers have collected about them and with a meaningful ability to have the information deleted, obscured, or corrected.



I. The Data Broker Ecosystem

Because data brokers typically have no direct relationship with the individuals whose data they collect, analyze, and sell, individuals are often unaware that brokers possess and sell information about them, let alone that they should read brokers' privacy policies.



As acknowledged by lawmakers, there exists an entire industry of companies comprising an “ecosystem of data brokers that purchase or collect data from web browsers and apps installed on Americans’ mobile devices” ([Warren, Maloney, Wyden, DeSaulnier Probe Data Broker’s Collection of Data on Black Lives Matter Demonstrators, 2020](#)). Data brokers vary widely in the scope of the services they offer and scale of the populations and data they cover ([Sherman, 2021a](#)). Unlike Big Tech companies, most of these brokers are not household names and most of their operations are not transparent to the public (see generally [Federal Trade Commission, 2014](#)). Brokers collect data from multiple sources, combine it in various forms, and then sell it commercially to buyers, which today increasingly include law enforcement and intelligence agencies ([Tau, 2021b](#)). Today, the data broker industry is reported to be worth upwards of \$200 billion, and data has been dubbed the “oil of the 21st century” ([Lazarus, 2019](#); [Toonders, 2014](#)).

There is no commonly agreed upon definition of what constitutes a ‘data broker’ and the term might often be used loosely ([Sherman, 2021b](#)). The California state legislature defines a data broker as “a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship” ([Assembly Bill No. 1202, 2019](#)). Vermont defines brokers similarly for purposes of establishing a state registry ([Protection Of Personal Information, 2019](#)). For purposes of this report, a data broker will mean any business that knowingly collects, purchases, analyses, or aggregates data used or intended to be used to identify individuals or their devices, without having direct relationships with those individuals, for the purpose of selling that data (see also: [Rieke et al., 2016](#); [Sherman, 2021a](#)).

The development of the data broker industry emerged from a lack of strong privacy protections. Data brokers provide a range of products for different purposes, some of which may be subject to regulation. For example, banks and credit unions may use information from data brokers for identity verification purposes as required by law, and in this context, the brokers are subject to regulation ([Federal Trade Commission, 2014](#)). More specifically, some data broker products used to support decision making on issues related to access to credit, insurance, housing, or employment are regulated by the Fair Credit Reporting Act (FCRA). However, the context in which data brokers are subject to specific regulations is the exception rather than the rule,

While these privacy concerns are relevant to all consumers, there are additional risks to specific groups. The use of data from data brokers and other technologies by law enforcement may also have disproportionate impacts on communities of color and immigrant communities in the U.S.

and the Federal Trade Commission explicitly has noted that there are many data-brokers that collect and sell data for purposes not covered by the FCRA (e.g., for marketing or locating people) ([Federal Trade Commission, 2012](#)).

Not only are the activities of data brokers generally unregulated, but the typical means of protecting privacy in the U.S. – the publication of privacy policies that ostensibly provide a mechanism for notice and consent – is especially unworkable in this context. Because data brokers typically have no direct relationship with the individuals whose data they collect, analyze, and sell, individuals are often unaware that brokers possess and sell information about them, let alone that they should read brokers’ privacy policies. Also, although data brokers or their clients may claim that some or all of the data in question is “anonymized”, it can often be re-identified when combined with other data.

The privacy concerns around data brokers are exacerbated because much of the data they collect and sell consists of sensitive personal information. There are various legal definitions of what constitutes sensitive personal information, such as under the California Consumer Privacy Act (CCPA) and the European Union’s General Data Protection Regulation (GDPR). Because the United States lacks a comprehensive consumer privacy law and U.S. legal doctrine is evolving, we use the term “sensitive” in this report to refer broadly to information that reveals details about an individual’s activities, associations, beliefs, communications, finances, health, patterns of travel, physical characteristics, sexual orientation, or other information that shows what the Supreme Court has referred to as “the privacies of life.”

While these privacy concerns are relevant to all consumers, there are additional risks to specific groups. For example, the use of data from data brokers and other technologies by law enforcement may also have disproportionate impacts on communities of color and immigrant communities in the U.S. One recent example of this is the case of a broker that obtained data from a Muslim prayer mobile app and in turn sold that to Immigration and Customs Enforcement ([Cox, 2021a](#)).

////

A. How brokers acquire data

While it’s not always clear how data brokers obtain data, they collect information from a multitude of sources ([Rieke et al., 2016](#); [US Senate Committee On Commerce, Science, and Transportation, 2013](#)), both private (e.g., financial institutions or employers) and public (e.g., government records), which can include data on devices, consumers, products, locations, or transactions ([Martin, 2015](#)). Data brokers can also purchase data from third-parties (or even other data brokers) who buy and aggregate data from many mobile app developers ([Keegan & Ng, 2021](#)). In many cases these mobile apps may share location and other personal data with third-parties and data


brokers without the knowledge of users of those apps ([Forbrukerrådet, 2020](#)).

Data broker Babel Street uses this approach with its “Locate X” data feed ([Levinson, 2020](#)), which offers historical device location data from geo-enabled advertising sources which may or may not be derived from cell site location information. The data broker Venntel indicates that it “collects and process[es] various types of information from mobile devices [from] third-party partners,” and this information can include “location data” associated with various advertising IDs ([Venntel, 2021](#)). The broker Giant Oak, Inc. indicates that it collects data from interactions with third party applications or features of websites, including social media, that allow third party connections (such as Facebook or Twitter); that data may include use information, IP addresses and other device identifiers, browsing histories, and may also involve cookies ([Giant Oak Inc., 2019](#)).

Brokers may also engage in scraping or ‘mining’ of publicly available data in order to repackage it, even though that may be prohibited by the terms of service of some social media companies ([Perez & Whittaker, 2020](#)). One such data broker is Clearview AI, which received cease and desist letters from several social networking companies regarding this practice ([CBS News, 2020](#)). Another example of a data broker that engages in significant scraping is Dataminr, which claims to mine 10,000 public data sets according to freedom of information documents obtained by Just Futures Law ([Mijente \[@ConMijente\], 2020](#)). Companies may provide analytics and services with data. For example, Dataminr provides an alerts system to law enforcement based on Twitter feeds, even though Twitter prohibits using its data for “tracking, alerting or monitoring sensitive events” ([Horwitz & Olson, 2020](#)).

Some data brokers assert that, while they provide certain types of sensitive data, the data has been de-identified or anonymized. For example, Babel Street’s Locate X service represents that “[t]he incoming data has been anonymized at the provider level through the assignment of a randomly designated device ID to each device. The Locate X Data Feed only provides access to data obtained from devices and does not have a direct correlation to identity” ([Babel Street, 2020b, pp. 2–3](#)). However, this is reportedly not true ([Cox, 2020](#)). Location data, even if it is de-identified (i.e. not directly tied to a specific customer profile) can be very difficult to anonymize ([Nojeim & Azarmi, 2020](#)). Indeed, according to one study, which used more than 15 months of

Location data, even if it is de-identified (i.e. not directly tied to a specific customer profile) can be very difficult to anonymize.



anonymized mobile location data of 1.5 million people, 95% of that cohort could be identified by merely four data points each ([de Montjoye et al., 2013](#)).

////

B. Data supply chains

Scholars of privacy and technology observe how “data, such as online consumer data or location data from an application is passed from one firm to the next within an information supply chain, comparable to supply chains in traditional industries” ([Martin, 2015, p. 70](#)). Just as traditional products may be manufactured at a factory, and then sent to processing facilities and then distributors to be sold, the data analytics (or ‘big data’) supply chain may consist of firms that interact with consumers and then sell data to tracking companies, which in turn provide it to data brokers. Information from brokers can then be used to place advertisements on websites, it may be employed by businesses to make strategic or employment decisions, or it may be utilized by researchers or government agencies ([Martin, 2015](#)). As a result, data supply chains are often highly attenuated, and privacy policies of data brokers contain language that permits, and often contemplates, attenuated sharing or purchasing of consumer data.

1. Data chains can be highly attenuated

A data broker is unlikely to be the entity that initially collected the data that it makes available commercially. In fact, data may often pass through several different providers before it finds its way to a data broker. Data may be purchased for one purpose, but ultimately repurposed for another, making preserving legal protections and accountability difficult.

In some instances, the data may be used or sold unbeknownst to the original provider. For instance, T-Mobile took the position that it was unaware that Securus Technologies, a major provider of correctional facility phone services, purchased real-time location information from major wireless carriers including T-Mobile and provided that information to the government ([T-Mobile, 2018](#)). T-Mobile described how its aggregator program, similar to that offered by national carriers, provides multiple aggregator partners “with access to customer location data” derived from network operations, and these partners in turn provide the data to “approved third party service providers who use such location data in providing various services” which might include proximity marketing, mobile gaming, product delivery, and other services.

Data brokers themselves may not contract directly with federal agencies, but may provide databases through different vendors. In some instances, a vendor who contracts with agencies may acquire data from other companies and may also provide its broker services through intermediary companies. For example, Venntel sells location data to

several federal agencies. It may also acquire data from other companies ([Tau, 2021c](#)), and it offers the same underlying data through another broker, Babel Street, which uses it in its Locate X product that it sells to several federal agencies ([Cox, 2021b](#)). Customs and Border Protection (CBP) has procured millions of dollars of Babel Street software contracts not through Babel Street directly, but through a Virginia-based government contracting vehicle called Panamerica Computers Inc., or PCi Tec.¹ Meanwhile, another Department of Homeland Security (DHS) component, Immigration and Customs Enforcement (ICE), contracts directly with Babel Street.²

2. Privacy policies of data brokers are often not transparent

Individuals do not disclose their digital information to businesses or other private parties in a vacuum, but often do so within a set of contractual rules called terms of use or privacy policies, which spell out when, how, why, and where information can be used ([Nissenbaum, 2009](#)). These terms may vary depending on the type of relationship, or might be governed by specific laws (such as health care information under HIPAA, or credit card information under the Fair Credit Reporting Act). However, there is no general federal privacy law in the United States, and hence in many contexts private policies (and general laws against unfair and deceptive trade practices) are the only protections that may apply. Individuals may maintain a set of expectations regarding their relationship with the first firm in a data supply chain, but have little or no knowledge of how that firm has shared data ‘downstream’ to aggregators or brokers, or how those downstream firms do, or do not, protect the privacy of that data. In some contexts, contractual provisions may limit the ability of data brokers to further share personal information,³ but in general, once brokers have obtained individuals’ information, the only protections come from the brokers’ own opaque privacy policies.

1 [Delivery Order HSHQDC12D00013-70B04C18F00001093](#) (CBP, \$2.3 million, Panamerica Computers, Inc., 2018-2019); [Delivery Order HSHQDC12D00013-70B03C20F00001148](#) (CBP, \$265k, Panamerica Computers, Inc. 2020-2021); Panamerica Computers, Inc., Partners, <https://www.pcitec.com/partners-1> [<https://perma.cc/A6XW-6BMA>].

2 [BPA Call 70CMSD19A00000007-70CMSD19FC0000052](#) (ICE, \$1.5 million, Babel Street, Inc., 2019-2021).

3 See Federal Trade Commission ([2021](#)) finding that when Internet Service Providers contract with data brokers to obtain services such as fraud detection, they often include contractual provisions that bar the brokers from further sharing consumers’ personal information that the ISPs provide in connection with those services.

Privacy policies of data brokers, particularly those that contract to provide data to law enforcement and intelligence agencies, generally contain subtle but carefully crafted language that contemplates commercial sharing with government agencies.




For example, in one review of the data sharing practices of a sample of medical apps on the Google Play store, researchers found that the app developer's privacy policies often allow for sharing user data with third-parties or brokers for analytical, advertising, or other purposes, and that the user's shared data would then be subject to the privacy policies of those third-parties. However, a review of the privacy policies of the third-parties found that they did not cover user data but instead focused on the treatment of the app developer's data (i.e., their client). Users were referred back to the app developer with regard to their specific privacy concerns ([Grundy et al., 2019](#)). These carve-outs for sharing user data with third-parties or brokers in the app's privacy policy may in fact mean that user data is subject to contractual privacy protections once the data is in the hands of a broker or other third party.

Privacy policies of data brokers, particularly those that contract to provide data to law enforcement and intelligence agencies, generally contain subtle but carefully crafted language that contemplates commercial sharing with government agencies. More importantly, individuals may not even have an opportunity to consent to this language, as there is almost always no transparency that a specific broker has obtained an individual's data and, thus, one would have no idea that a given privacy policy applies (see for example [Giant Oak Inc., 2019](#)).

For example, Babel Street's privacy policy broadly prescribes that it may use "information given to us by customers and other individuals, such as referrals or other contacts" ([Babel Street, 2021b](#)). The scope of "other individuals" or "other contacts" potentially captures any possible source. The policy also delineates that the company may share information "where we have a legal obligation or authorization and/or legitimate interest to do so." There is no clarity as to what a "legitimate interest" may entail.

The data broker SkyHook provides various location-based services and indicates it may comply with any "government request received by Skyhook, whether or not a response is required by applicable law" ([Skyhook, 2021](#)). Finally, Venntel, which collects various forms of location data, advertising IDs, IP address information, and "other device information" indicates that it may share all of that information with customers for purposes of "federal law enforcement" and "national security," and that Venntel's customers "may also resell your information to other third parties for similar purposes" ([Venntel, 2021](#)).



II. Legal Framework

A complex legal framework in the United States governs law enforcement and intelligence-based access to data. Among other things, this framework subjects certain location-based information to the Fourth Amendment’s warrant standard. However, the government is exploiting loopholes in the framework by purchasing data from private data brokers. This report briefly evaluates some key aspects of this framework in order to contextualize the analysis of data brokers, but does not attempt to be exhaustive.

////

A. The loophole in the Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act of 1986 (ECPA) was passed to limit the government’s ability to access digital communications, or information about such communications, without adhering to certain legal standards. It achieved this by defining categories of electronic service providers (covered entities) whose customer records are subject to heightened protections. However, ECPA does not reference modern data brokers, which did not exist in the 1980s. As one commentator observed, “[w]hile much of the ECPA was ahead of its time, other parts haven’t aged as well” ([Kalat, 2019](#)).

Providers are required to safeguard customer records by not knowingly disclosing those records to third parties under various circumstances. ECPA provides a framework for the who, what, and when of permitted disclosure that varies based on a number of factors. ECPA provides for two categories of covered services (see 18 U.S.C. §§ 2510(15), 2711(2)):

1. A Remote Computing Service (RCS), or the “provision to the public of computer storage or processing services by means of an electronic communications system.”
2. An Electronic Communication Service (ECS), which is “any service which provides to users thereof the ability to send or receive wire or electronic communications.”

Subject to certain exceptions, an ECS provider is prohibited from disclosing to third parties “the contents of a communication while in electronic storage by that service,” while an RCS provider cannot disclose “the contents of any communication which is carried or maintained on that service” (18 U.S.C. §§ 2702(a)(3)). With respect to disclosure of non-content information to the government, both RCS and ECS providers are prohibited from “knowingly divulg[ing] a record or other information pertaining to a subscriber to or customer of such

service . . . to any governmental entity” unless an exception applies (18 U.S.C. § 2702(a)(3)). This would also prohibit the sale of such information by ECS or RCS providers to the government.

If the government wishes to access customer information held by an RCS or ECS, ECPA provides a specific legal process that must be followed. The government can obtain subscriber information, such as name, address, and phone number, by issuing a subpoena under Section 2703(c)(2). In order to obtain other “non-content” information that is more sensitive than subscriber information, such as traffic or transactional information, the government must obtain a Section 2703(d) order. Such orders compel a provider to disclose certain “non-content” information when the government is able to demonstrate “specific and articulable facts showing that there are reasonable grounds to believe” that the information is “relevant and material to an ongoing criminal investigation.”⁴ This standard is much less stringent than the probable cause requirement to obtain a search warrant under the Fourth Amendment. Finally, when the government seeks to obtain the content of electronic communications, the government must obtain a warrant supported by probable cause (see *United States v. Warshak*, 2010) and also (*Carpenter v. United States*, 2018).

It may often be unclear whether a service is an ECS or RCS. Many providers perform both functions, as well as services that are neither ECS or RCS services. Courts have held that WhatsApp, for instance, is an ECS (*United States for PRTT Order for One Whatsapp Chief Account for Investigation of Violation of 21 U.S.C. § 841*, 2018). However, how other services are classified may depend on the capacity in which they collect data, and whether it is in the context of messaging or data storage. There is a question as to whether “content” can include location or proximity data where the very purpose of a service is to record or communicate location or proximity data. For example, Google has taken the position that data ‘Location History’ feature is “content” of communications for purposes of ECPA (*Google Amicus Brief*, 2019). However, in most cases where devices and apps record location information, it has been considered to be “non-content” information.

ECPA permits RCS and ECS providers to *voluntarily* provide non-content information to non-government third parties. If those third parties are not RCS or ECS providers themselves, ECPA does not apply and accordingly does not prohibit them from selling or otherwise providing the information to the government. This gap has enabled ECS and RCS providers to transfer data voluntarily to private third parties who are not

⁴ Prior to the Supreme Court’s decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the government was able to obtain cell site location information (CSLI) through a Section 2703(d) order, but the *Carpenter* Court held that in order to obtain such information for a period of seven days or more, the government is required to show probable cause and obtain a warrant.

covered by ECPA, and then those third parties have been able to sell the data to data brokers or directly to government agencies. This creates the ECPA loophole that has allowed government agencies to purchase sensitive information from data brokers even though those agencies should have been required to obtain a warrant, a court order, or a subpoena under ECPA.

////

B. The Supreme Court recognized the sensitivity of device location information in *Carpenter*

Under longstanding Fourth Amendment doctrine, when individuals have a “reasonable expectation of privacy” in certain information, the Fourth Amendment generally requires the government to obtain a warrant in order to access that information (*Katz v. United States*, 1967). Over the past decade, the Supreme Court has increasingly recognized that people possess a “reasonable expectation of privacy” in much of their personal digital information. Thus, by purchasing certain personal data of Americans from brokers, law enforcement and intelligence agencies are side-stepping not only ECPA, but also Fourth Amendment safeguards, as recognized by the Supreme Court in the 2018 landmark case *Carpenter v. United States*. Although the Supreme Court stated that its holding in *Carpenter* was narrow, the language of the opinion suggests that the government must obtain a warrant in order to access sensitive personal information in contexts beyond the facts of the case.

In *Carpenter*, the Court held that a warrant is required for law enforcement to access historical cell site location information (CSLI) for a period of seven days or more. The opinion analyzed at length the significant privacy interests in digital information that reveals one’s life and beliefs, particularly location information. Ultimately the Court applied that premise to guarantee more robust protection for location information traced to cell phone movements, finding that the standard for acquiring location information in ECPA did not provide adequate safeguards for the Fourth Amendment interests at stake. The Court specifically recognized that location information “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’” (*Carpenter v. United States*, 2018, p. 2217). The Court also noted that the collected location information was “detailed, encyclopedic, and effortlessly compiled.”⁵ Thus, *Carpenter* provided that a warrant was required to obtain seven days or more of historical cell-site location information from a wireless carrier.

The specific facts of *Carpenter* involved cell tower-source geolocation information (rather than GPS), location information that was stored, and collected over a period of at least a week, as well as used in law enforcement (rather than intelligence) investigations. Nonetheless, the Court’s reasoning surrounding the privacy concerns

5 The Court referred to its earlier decision in *United States v. Jones*, 132 S. Ct. 945 (2012).

The Court's reasoning surrounding the privacy concerns of location data strongly suggest that collection of a multitude of sensitive digital information – not simply location data – is also covered by the Fourth Amendment's warrant requirement.

of location data strongly suggest that collection of a multitude of sensitive digital information—not simply location data—is also covered by the Fourth Amendment's warrant requirement. Many forms of private digital information beyond location implicate the 'familial, political, professional, religious, and sexual associations' and the "privacies of life" that the Supreme Court recognized a paramount privacy interest in safeguarding. In addition, although the *Carpenter* opinion explicitly stated that application to foreign affairs and national security remained an open question, the *Carpenter* analysis "focuses on the privacy interest at stake and provides no basis for distinctions premised on the purpose of the search" ([Franklin, 2018](#)).

Internal legal justifications of government purchases of sensitive data from data brokers—from both law enforcement (DHS) and intelligence agencies (DIA)—are explicit in referencing *Carpenter* and stating that they believe the case does not apply to their practice (see for example [Defense Intelligence Agency, 2021](#)). However, in our view, the broad language of the *Carpenter* opinion indicates that its holding should apply in the national security context and to other categories of sensitive data. Thus, even though the Fourth Amendment does not restrict the activities of data brokers (unless they are state actors in a particular context), government agencies that purchase location and other sensitive digital data without a warrant may well be violating the Fourth Amendment.

////

C. Legal considerations for intelligence agencies

Legal interpretations and frameworks applicable to intelligence agencies reference the commercial acquisition of data from private vendors. Generally speaking, intelligence activities are governed by Executive Order 12333, which lays out the structure and legal framework for intelligence collection, including the collection of information on U.S. persons if certain criteria are met. Under Section 2.3(a) of the Executive Order, one of those criteria is that the information is "publicly available information" (PAI) (*Exec. Order No. 12333, 1981*).

The Defense Intelligence Agency's position is that *Carpenter's* scope is limited to law enforcement actions and does not prohibit the intelligence community's authority to collect commercially available information ([Defense Intelligence Agency, 2021](#)). In arguing this, the agency stated that the opinion "expressly did not consider collection techniques involving national security." However, as outlined above, the privacy interest at stake, rather than the purpose of the search, formed the basis of *Carpenter's* analysis.

It is worth noting that even where constitutional limits preclude U.S. government agencies from engaging in certain types of collection, legal doctrine under the U.S. Constitution does not constrain foreign governments. Intelligence agencies may

argue that they should not be barred from purchasing data from private data brokers if foreign adversaries are freely able to make such purchases to acquire sensitive data about Americans. However, access by foreign governments does not justify an evasion of constitutional safeguards. Instead, policymakers should consider how to address the ability of data brokers to sell sensitive information about Americans to foreign adversaries. It is also not clear whether, and to what extent, U.S. intelligence agencies may be sharing data purchased from data brokers with foreign allied governments, and policymakers should evaluate such foreign sharing as well.

Each of the 17 components of the Intelligence Community issues its own guidelines – which must be approved by the Attorney General and are typically referred to as “Attorney General Guidelines” – which govern collection and use of information on U.S. persons under E.O. 12333, so interpretations as to the scope of *Carpenter* may vary. The Attorney General Guidelines provide a framework for collection of information considered to be publicly available, which generally does not require special approvals to acquire, and which may explicitly include commercially acquired information (see for example, [Office of the Director of National Intelligence, 2020](#), p. 12, 31).

////

D. Overbroad and misleading use of terms ‘open source’ and ‘publicly available’

As outlined previously, the Fourth Amendment generally requires the government to obtain a warrant in order to access information in which individuals have a reasonable expectation of privacy, and statutes such as ECPA require the government to use legal process to obtain certain types of data held by communications service providers. Conversely, if people freely make information available to the general public, they lack any protected privacy interest in such information, and government agencies can collect such data without obtaining a warrant or other legal process. On this basis, government agencies are permitted to collect ‘publicly available’ information without seeking a warrant or other legal process.

However, law enforcement and intelligence agencies obtain from data brokers information that may not be actually available to individuals in the public. Agencies use terms such as ‘open source’ or ‘publicly available’ in conjunction with solicitations for contractors to collect certain sensitive information such as location data obtained specifically for purposes of that contract. For example, the FBI indicates in one solicitation document (see Figure 1) that it is “optional but advantageous” to have “GPS information if available open source.”⁶ The U.S. Army Criminal Investigation Command (USACIDC) refers to open source to mean “publicly available information”

⁶ Solicitation 15JPSS19R00000013, pp. 24-32 et seq. (FBI, Computer Assisted Legal Research 5, 2018); [full document pages [1-50](#) / pages [51-104](#)].

in conducting market research of company capabilities.⁷ It is critical to note that these phrases may not have uniform definitions across government agencies, and it is worth scrutinizing precisely what is meant by them. Information characterized as “open source” or “publicly available” may not in fact be readily available to the public, and may require specialized companies to conduct research and collect data specifically to meet the terms of a government contract.

C.9.4.1.13 Internet and Social Media Footprint

Query	Results	
Searchable by	Required but not limited to	Optional but advantageous
<ul style="list-style-type: none"> - Name - Address - Phone number 	<ul style="list-style-type: none"> - Email address - IP address profile - Screen-name - Online associates - Forum presence - Social media presence (Facebook; LinkedIn...) 	<p>All possible Internet Footprint data; Data used to create user accounts (phone number; email; name); GPS information if available open source; Likes; groups; Mobile phone platform media snapchat; Instagram); Monikers; resumes; CVs; news articles; P2P; Phone applications; possible; Photos; Server information; Static; Dynamic; mobile; Hotspots; Twitter; Tumblr; Snapchat; User ID (this stays the same even if the User Name Changes); WhatsApp; BBM; etc.; wish lists and registries; Alternate communication tools (telegram; WhatsApp; Viber; etc...)</p>

Figure 1. Illustration of how the term “open source” is used in some solicitations. Source: FBI (2018) Computer Assisted Legal Research 5, ([Solicitation 15JPSS19R00000013](#)) - pg. 28.

For some agencies, publicly available information, or PAI, explicitly covers commercially available data. The Department of Defense, for purposes of defense intelligence activities, defines PAI as including “information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase” ([Department of Defense, 2016](#)). The Office of the Director of National Intelligence (ODNI) Attorney General Procedures for Conducting Intelligence Activities (Attorney General Guidelines), outline the core framework for ODNI’s collection and handling of information concerning U.S. persons. The Attorney General Guidelines define public availability in similar language, with the caveat that “commercially acquired data” may only be considered publicly available if non-U.S. government persons or corporations could acquire the data from the same source. The CIA has also adopted rules outlining what information may be considered to be publicly available

⁷ Memorandum for Record – Limiting Competition at or below the Simplified Acquisition Threshold - [Modification # P00005 to existing Contract # W15QKN-15-C-0111](#).

([CIA, 2017](#); [Kris, 2017](#)). Unfortunately, other agencies may not limit the data they purchase to information that members of the public might actually find to be available to them. Thus, it is possible that “commercial acquisitions of data may be so tailored and specialized for government use, and unavailable to a similarly situated private-sector purchaser, that the data cannot be considered publicly available” ([Office of the Director of National Intelligence, 2020](#), p. 31).

This is not to say that the terms ‘open source’ or ‘publicly available’ always misleadingly designate commercially acquired data unavailable to private purchasers; by the same token, these terms in government purchase orders and contracts do not automatically preclude commercial acquisition of data that as a practical matter is available only to the government.



III. Federal Agency Use Cases for Brokered Data

In our review of publicly available documents of law enforcement and intelligence agency Requests for Proposals (RFPs) for data broker products, we found 30 awards valued at approximately \$86 million in total. This is a very small proportion of the actual number and overall value of these transactions since information about such transactions can be difficult to obtain. Moreover, the number of transactions understates the use of commercially acquired data because agencies also frequently share data that is obtained; Forensic Logic’s COPLINK X, for instance, utilizes 3225 individual data sources and a billion law enforcement records, bi-directional interfaces to feed and retrieve data to and from federal repositories among all its clients.⁸

The documents suggest that data obtained from brokers are employed for a variety of purposes such as pre-investigative inquiries, intelligence gathering, crime prevention, or criminal investigations. Indeed, commercially acquired data feeds into the data-driven operation of modern law enforcement and intelligence ([Rieke et al., 2016](#), p. 34), a phenomenon which scholars have called “big data policing” ([Ferguson, 2019](#); [Lamdan, 2019](#)). Moreover, this trend appears to be increasing, and Congress is pressing the intelligence agencies to elevate the importance of, and increase reliance on, “open-source” information ([Aftergood, 2021](#)).

Law enforcement and intelligence agencies obtain numerous forms of data commercially where, as we explained above, legal process should be required, or where the original provider is precluded from disclosing information directly to the government under ECPA. As noted above, the data collected and sold by data brokers includes various types of sensitive data (e.g., health data, travel patterns, financial information, etc.). We focus here on the types of data that law enforcement and intelligence agencies generally seek to purchase from brokers, including mobile device geolocation data, communications data and metadata, and license plate reader (LPR) data.

////

A. Mobile device geolocation data

Geolocation data generated by operation of a mobile device entails latitude-longitude coordinates that can be derived from numerous sources, including GPS, cell tower triangulation, WiFi connection data,

⁸ [Sole Source Procurement Justification](#) (Dona Ana County Sheriff’s Department, \$45.5k, Forensic Logic LLC, 2020-2021).

or other techniques. Geolocation data is often associated with a mobile advertising ID, or a unique user-resettable identifier that tracks the user's behavior and usage of apps. This ID allows advertisers to personalize ads delivered to that user. It's essentially the mobile application equivalent of a third-party web browser cookie, which is also used to track user activities. The two main mobile advertising IDs are Apple's Identifier for Advertisers (IDFA) and Google's Advertising ID (GAID)/Android Advertising ID (AAID).⁹ Location-based marketers view geolocation data as a "key ingredient for marketers in reaching consumers in their increasingly connected day-to-day lives," pointing out in 2019 that 82% of marketers had utilized location data to personalize customer experiences, and even more planned to do so in the future ([Factual, 2019](#)).

Various locales including retail stores, airports, and hotels use Mobile Location Analytics (MLA) technology to understand aspects like traffic or where customers spend the most time browsing. "MLA works by detecting a device's WiFi MAC or Bluetooth address, which is a twelve-digit alphanumeric string assigned to the device by manufacturers" ([Future of Privacy Forum, 2016](#)). Geolocation data utilized in ad-tech does not necessarily leverage the precise location built into mobile operating systems—such as GPS, cell site location data, and WiFi networks—and much location data used is consequently inefficient ([Williams, 2019](#)). Although brokers may compile this data in order to sell it for such commercial uses, as described below, government agencies have also sought to purchase this information, including for law enforcement purposes. For example, although Mobilewalla asserts that its business model does not focus on sales to law enforcement, it acknowledged in November 2021 that it had been the source of mobile device data used by DHS, the IRS, and other government agencies to track mobile phones without warrants ([Tau, 2021c](#)).¹⁰

Law enforcement location analysis is sometimes called "location intelligence" and may be used in multiple law enforcement contexts beyond simply crime analysis; numerous agencies put significant resources into geolocation analysis.

Location, particularly digital locations derived from mobile devices, can constitute a critical component of modern criminal investigations. Marketing materials for location analytics provided by the Environmental Systems Research Institute (ESRI), a company providing geographic information system (GIS) software and support, emphasize how "[o]ne of the foundations of criminological theory is that three things are needed for a crime to occur: a motivated offender, a suitable target, and a location" ([ESRI, 2017](#)). Law enforcement location analysis is sometimes called "location intelligence" and may be used in multiple law enforcement contexts beyond simply crime analysis;

⁹ Note that Apple has added an option for consumers to opt-out these forms of tracking. See <https://developer.apple.com/app-store/user-privacy-and-data-use/> [<https://perma.cc/Y364-E2H8>]. Google has implemented a similar option as well: <https://support.google.com/googleplay/android-developer/answer/6048248?hl=en> [<https://perma.cc/QCT2-6MD3>].

¹⁰ Further, news reporting indicates that law enforcement and intelligence agencies have sometimes sought data sets outside of the federal contracting process through voluntary productions by employees of digital marketing and location analytics companies ([Tau, 2021c](#)).

numerous agencies put significant resources into geolocation analysis.¹¹ For example, one geofencing search warrant indicates how “[l]ocation data can assist investigators in understanding a fuller geographic picture and timeline by identifying the cellular telephones in the area during the offenses described” (*Affidavit, Search of Information on Computer Servers Controlled by Google, Inc.*, 2018). This has the effect of “possibly inculcating or exculpating account owners,” which has simultaneously led to privacy concerns over the impact of the practice on bystanders ([Note, 2021](#)).

The FBI has publicly acknowledged that it utilizes commercially-obtained data in pre-investigative activities. While the FBI does not discuss or disclose investigative techniques, a picture of various uses of commercially-obtained data can be pieced together from various public sources. The FBI may, pursuant to the 2008 Attorney General’s Guidelines on Domestic FBI Operations, open an “Assessment” on any individual or organization without a criminal predicate. An assessment is a pre-investigative stage, and according to FBI documents can include searching “commercial and government databases.” Location data from commercial sources may also be utilized ([German & Hockett, 2017](#)). The FBI has contracted with the data broker Venntel as well as another firm to access Venntel’s portal ([Fang, 2020](#)).¹² Venntel sells location data harvested from a variety of sources including ordinary apps. In the Venntel system, agencies can access a panel where users view the locations of smartphones over time, with data sourced from many companies and ad firms, as well as apps including weather apps.

Customs and Border Protection (CBP) also contracted with Venntel in 2020. Reportedly, CBP could use the technology to identify specific people, searching an area “to look for devices in that particular place, or by looking up an identifier of a specific device” ([Cox, 2020](#)). DHS also has contracted with Venntel to purchase ‘geographic marketing data,’ though it is unclear what is contained in this ‘geographic’ data.¹³

Thomson Reuters, a Canadian company and one of the world’s largest data aggregators with revenue of more than \$5 billion annually ([Thomson Reuters, 2021](#)), has contracts worth tens of millions of dollars with law enforcement agencies for a multitude of purposes, including location tracking, and it continues to maintain contracts with

11 E.g. in June 2020 the FBI entered into a \$4.3 million one-year contract with ESRI for ArcGIS products and services. [BPA Call 15F06718A0008180-15F06720F0002074](#) (FBI, \$4.3 million, Environmental Systems Research Institute, Inc., 2021); DHS maintained a contract of nearly \$2 million through 2021 with Ardent Management Consulting Inc. for “geospatial data and operational support.” [BPA Call HSHQDC16A00005-70RTAC19FC0000065](#) (DHS, \$1.3 million, Ardent Management Consulting, Inc. 2019-2021). See also ([Tau, 2020](#)).

12 See [Delivery Order NNG15SC77B-15F06720F0000659](#) (FBI, \$22.3k, Govplace Inc., 2020-2021).

13 [Delivery Order HSHQDC12D00013-70RSAT18FR0000172](#) (DHS, \$671k, Panamerica Computers, Inc., 2018-2019); [Delivery Order HSHQDC13D00022-70RSAT18FR0000052](#) (DHS, \$362k, Govplace, Inc., 2018-2019).

numerous law enforcement and intelligence agencies ([Thomson Reuters, 2019](#)).¹⁴ Thomson Reuters Special Services (TRSS), LLC, a specialized U.S. subsidiary of Thomson Reuters which provides “strategic and tactical global risk insights,” ([Thomson Reuters, n.d.-a](#)) offers numerous databases including the Consolidated Lead Evaluation and Reporting (CLEAR) database. A sole source justification from the Marine Corps Intelligence Surveillance Reconnaissance Enterprise references CLEAR’s ability to provide a “live gateway” to “cell phone data.”¹⁵ The extent and scope of this “cell phone data” is not readily apparent. ICE indicated that TRSS’ proprietary services “will allow the agency to quickly build a full picture of a person of interest through finding contact and location information, identifying associations, making connections between individuals, activities, locations, and more with the most recent and relevant information updated frequently.”¹⁶ The Department of Treasury Office of Intelligence and Analysis also contracted with CLEAR beginning in 2021.¹⁷

Similarly, the RELX Group, which provides LexisNexis Accurint law enforcement services, has entered into contracts worth over \$10 million with CBP, ICE, the Secret Service, and Citizenship and Immigration Services.¹⁸ RELX also owns ThreatMetrix, a cybersecurity company that tracks users online; LexisNexis ThreatMetrix advertises its “first layer of defense” to include “web & mobile device intelligence” as well as “true geolocation” ([LexisNexis, 2021a](#)). As part of this, Lexis advertises its Digital Identity Network which boasts the following capabilities:

The LexisNexis® Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments, and new account applications. Using this information, the ThreatMetrix solution creates a unique digital identity for each user by analyzing the myriad connections between devices, locations, and anonymized personal information. ([LexisNexis, 2021a](#))(PDF download).

14 As a result of CLEAR, among other things, pressure has mounted on the company from shareholders to re-examine its contracts ([Dang & Kerber, 2021](#)).

15 [Sole Source Justification M0009619SUINS07](#) (Marine Corps Intelligence Surveillance Reconnaissance Enterprise, Thomson Reuters, 2019); [Limited Source Justification and Approval](#) (Naval Supply Systems Command, Thomson Reuters, 2021).

16 Office of Acquisition Management, [Sole Source Justification, J&A-19-0208](#) (DHS, ICE, OAO, IOSD, OPR, \$3.4 million, Thomson Reuters Special Services LLC, 2019-2021); [Definitive Contract 70CMSD21C00000002](#) (DHS, \$4.2 million, Thomson Reuters Special Services LLC, 2021-2026).

17 Special Notice to [Sole Source 2032H321N00072](#) (OIA, Thomson Reuters, 2021).

18 Delivery Order [LC14C7121-70B04C18F00000031](#) (CBP, \$8.8 million, RELX Inc., 2017-2021); Delivery Order [03310319D0028-70SBUR19F00000548](#) (Citizenship and Immigration, \$484k, RELX Inc., 2019-2020); Delivery Order [03310319D0028-70CDCR20FR0000053](#) (ICE, \$115k, RELX Inc., 2020-2021); Delivery Order [03310319D0028-70US0920F30TH0082](#) (Secret Service, \$830k, RELX Inc., 2020-2022).

Lexis also offers a “ThreatMetrix for Government” product which boasts the ability to provide “locations” and “past online/location behavior” (See Figure 2).¹⁹ Brochures as well as a Lexis federal supply schedule indicate that the service can provide real-time location and device intelligence. The service further advertises: “ThreatMetrix for Government provides the fast, digital identity assessment agencies need. It harnesses data intelligence about devices, locations, identities and past behaviors across one of the world’s largest, crowdsourced, global digital networks. The result is government agencies know who they’re transacting with, reducing access from fraudsters and bots” (LexisNexis, 2021b). While agencies may not typically list the specific databases they purchase from a vendor in procurement records, ICE has previously referenced ThreatMetrix by name in a \$112.5k contract award acquired through the FirstSource II contract vehicle.²⁰

Digital Identity and Physical Identity	
Digital Identity (ThreatMetrix Data)	Physical Identity (Public Records)
Devices and phone numbers associated with devices	Address, zip code, lifestyle
Locations	Vehicles (car, plane, boats)
Past online/location behavior	Property
Logins	Professional Licenses (nurse, doctor)
Types and frequency of transactions (payments and new account creations)	Education credentials; Owner of a business
Billing and shipping address	Public records and other data linked with a unique identifier (LexID)

Figure 2. Data available from the “ThreatMetrix for Government” service. Source: LexisNexis, [Authorized Federal Supply Schedule Pricelist, GS00F178DA](#), 2016-2021, p. 9.

The FBI also seeks certain GPS Internet and social media footprint information from companies like Thomson Reuters and RELX Group. In a solicitation for “Computer Assisted Legal Research 5” or “CALR 5,” a category typically awarded to these companies, the FBI lays out in some detail the capabilities it seeks. Desired capabilities include a large number of personal data points, including social security number, address, date of birth, citizenship, and marital status. Other forms of data include phone data, utility records, and data points on businesses. However, the FBI also indicates it is “optional but advantageous” to have “GPS information if available open source.”²¹ As noted previously, it is unclear what the FBI considers to be open source,

¹⁹ LexisNexis, Authorized Federal Supply Schedule Pricelist, GS00F178DA, 2016-2021, p. 9.

²⁰ Delivery Order HSHQDC13D00015-HSSCCG17J00139 (ICE, \$112.5k, FirstSource II, 2017-2018).

²¹ Solicitation 15JPSS19R00000013, pp. 24-32 et seq. (FBI, Computer Assisted Legal Research 5, 2018); [full document pages [1-50](#) / pages [51-104](#)].

and whether it views obtaining location information commercially from brokers as ‘open source’. It is also unclear whether the FBI considers ‘open source’ to include data compiled specifically for the FBI to purchase, even where no other customer would actually be able to find or purchase that information. For example, in the same solicitation, the FBI sought the ability that “searches must remain non-attributable” and “untraceable.”²² This language suggests that the FBI was seeking a tailored product, rather than a dataset that might actually be available for purchase by private entities or the general public.

The DEA, from 2020 to 2021, has signed numerous contracts with the data broker Babel Street; the IRS, the Treasury Department’s Office of Foreign Assets Control (OFAC) ([Biddle, 2021](#)), the Secret Service, and ICE have also utilized Babel Street.²³ One of Babel Street’s software solutions, Locate X, which it offers as a standard service, provides “historical digital device location data” derived from “geo-enabled advertising sources,” or popular mobile apps ([Babel Street, 2020b](#); [Levinson, 2020](#)). The company has been secretive about the capabilities program, making users agree to not cite the product as a basis for legal process (see Figure 3) ([Babel Street, 2020a](#), p. 9). One DEA contract with Babel Street for \$220k merely references “data collection.”²⁴ Babel Street advertises that it runs an AI-enabled “analytics platform” which allows for search of thousands of PAI (publicly available information) sources in over 200 languages, although again it is unclear what is meant by ‘publicly available.’ The firm indicates that this information can be used to “discover and decipher insights” on persons of interest ([Babel Street, 2021a](#)).

22 Solicitation 15JPSS19R00000013, pp. 24-32 et seq. (FBI, Computer Assisted Legal Research 5, 2018), pg 32; [full document pages [1-50](#) / pages [51-104](#)].

23 Definitive Contract [70US0919C70090057](#) (Secret Service, \$2 million, Babel Street, Inc., 2019-2020); BPA Call [DJF161200S0009106-15DDHQ20F00001467](#) (DEA, \$220k, Babel Street, Inc., 2020-2021); BPA Call [70CMSD19A00000007-70CMSD19FC0000052](#) (ICE, \$1.5 million, Babel Street, Inc., 2019-2021).

24 BPA Call [DJF161200S0009106-15DDHQ20F00001467](#) (DEA, \$220k, Babel Street, Inc., 2020-2021).

- 2. Locate X Data.** Babel Street shall provide the Locate X Data to Customer pursuant to the terms of the applicable Order Form. For avoidance of doubt, Locate X Data constitutes a “Data Feed” as defined in the Terms and, as such, shall be subject to the applicable Terms. In addition, the following additional terms shall also apply to the Locate X Data:
- 2.1. The existence and terms and conditions of this Addendum, and the Locate X Data in its entirety, shall be considered “Confidential Information” of Babel Street subject to the Terms. In addition, notwithstanding Section 9.1 of the Terms, Locate X Data may not be disclosed by Customer to any third party (including consultants, advisors, and/or independent contractors) without the prior written consent of an authorized representative of Babel Street; and
- 2.2. Any and all Locate X Data, including, but not limited to, results generated by Customer’s use of the Locate X Data, will be used for internal research purposes only. Locate X Data may not be used as the basis for any legal process in any country, including as the basis for a warrant, subpoena, or any other legal or administrative action (nor may the Locate X Data be cited in any court/investigation-related document).

Figure 3. Segment from Babel Street’s User Agreement for Locate X. Source: ([Babel Street, 2020a](#), p. 9).

ICE in 2020 sought the ability to “[g]eo-locate individuals beyond standard geo-tagging,” explaining that “[t]he government defines geo-locating as the ability to provide a specific location of the subject/threat actor.”²⁵ It also sought the “[a]bility to determine (via publicly facing information) which social media websites were accessed by users prior to making a threat [toward a senior ICE employee],” although it is unclear what ‘publicly facing’ is restricted to, and its data sources also include “available proprietary sources,” meaning that this information could be commercially sourced.²⁶ Further, law enforcement and immigration enforcement monitoring of individuals’ social media usage raises a variety of serious civil liberties and civil rights concerns, including chilling free speech ([Brennan Center for Justice, 2019](#)).

Intelligence agencies, including the Defense Intelligence Agency (DIA), have also reportedly purchased commercial databases containing location data from smartphone apps and searched them for the past movements of Americans without a warrant ([Savage, 2021](#)). While commercially available databases may be initially purchased in order to acquire location data for investigations regarding foreigners outside the United States, the databases may not necessarily separate the data of U.S. persons from non-

²⁵ Solicitation [70CMSW20R00000002](#) (ICE, 2020).

²⁶ Solicitation [70CMSW20R00000002](#) (ICE, 2020), pg 5.

U.S. persons. Although the Intelligence Community has not released information regarding whether and to what extent other intelligence agencies may purchase information from data brokers, the DIA has publicly stated that it does so, and takes the position that it “does not construe the Carpenter decision to require a judicial warrant endorsing purchase or use of commercially available data for intelligence purposes” ([Savage, 2021](#)).

////

B. Communications data and metadata

Babel Street offers Locate X as a standard service, which provides historical location data obtained from advertising sources; however, the firm offers for “select” customers, “pending approved use cases,” the opportunity to use “Locate X Premium.” The Premium version “offers access to additional metadata and is an add-on purchase to Locate X” ([Babel Street, 2020b](#)). It is not defined what metadata is included in addition to, but associated with, device location data ([Cox, 2021c](#)). The Secret Service, Drug Enforcement Administration, and ICE have all utilized Babel Street,²⁷ although it is unclear whether agencies subscribe to Locate X Premium in addition to the standard Locate X service.

One solicitation by ICE seeks the capability to “identify whether a user has deleted messages and provide content from deleted accounts and/or deleted messages where applicable.”²⁸ Deleted messages would no longer be public-facing or publicly available; if law enforcement sought that information from a service provider, it would thus likely need a warrant. The social media sources sought to be covered include Facebook, Instagram, Twitter, Snapchat, LinkedIn, Tumblr, YouTube, Flickr, and Pinterest, among others, and the solicitation states that the capability should include the ability to “[m]onitor and analyze all social media activities . . . in REAL-TIME,” with the emphasis on ‘real-time’ occurring in the original document.²⁹ That \$2.1 million contract, with a potential value of \$5.5 million, was ultimately awarded to Barbaricum LLC, for a duration of five years from March 2020.³⁰ Barbaricum is an “all-inclusive government contracting firm” that is partnered with Palantir, which provides various services including analytical support and data integration ([Barbaricum, 2021](#); [Palantir, 2021](#)).

27 Definitive Contract [70US0919C70090057](#) (Secret Service, \$2 million, Babel Street, Inc., 2019-2020); BPA Call [DJF161200S0009106-15DDHQ20F00001467](#) (DEA, \$220k, Babel Street, Inc., 2020-2021); BPA Call [70CMSD19A00000007-70CMSD19FC0000052](#) (ICE, \$1.5 million, Babel Street, Inc., 2019-2021).

28 Solicitation [70CMSW20R00000002](#) (ICE, 2020).

29 Solicitation [70CMSW20R00000002](#) (ICE, 2020), pgs. 4-5.

30 Definitive Contract [70CMSW20C00000001](#) (ICE, \$5.5 million, Barbaricum LLC, 2020-2025).

A 2020 solicitation by an FBI field office for social media alerting capabilities sought “early alerts on ongoing national security and public safety-related events through lawfully collected/acquired social media data.”³¹ It went on to seek “[t]he mission-critical capitalization of open source social media data from multiple platforms” and in response to follow-up questions from vendors regarding what data sources should be used, indicated that “[v]endors are encouraged to provide the most comprehensive data sets available.”³² That request led to a five-year \$3.2 million contract, potentially worth up to \$14.1 million, for ZeroFox software.³³ ZeroFox is a threat analytics platform that includes coverage for top social networks like Facebook, Twitter, Instagram and LinkedIn ([ZeroFox, 2021](#)). The company indicates that it acquires data from “third party data providers” and promises that it takes “steps to ensure that such third parties are legally permitted” to disclose the data ([ZeroFox, 2020](#)). However, this commitment does not address the other end of the equation, whether a potential buyer (i.e. the government) is legally permitted to purchase the data. Further, government agencies have taken the position that it is legal under *Carpenter* to commercially acquire data that would otherwise require a warrant or process such as a 2703(d) order. Thus the phrase “lawfully collected” is one that should be scrutinized and not assumed to exclude data that would ordinarily require legal process to access.

A Marine Corps publication indicating an intent to contract with Thomson Reuters CLEAR describes a “significant differentiator” of the CLEAR service is its ability to provide “[l]ive gateways to real-time data from primary source and unique data only available to CLEAR, such as cell phone data, carrier data, and utility records.”³⁴ It is unclear what the scope of this real-time cell phone data entails, and whether it includes communications, although various divisions of the Marine Corps have since contracted with CLEAR.³⁵

////

C. License plate reader (LPR) data

Automated license plate readers (ALPRs) are computerized camera systems that capture all license plate numbers that come into view, recording the location, date, time, as well as photographs of the vehicle and, at times, drivers and passengers. ALPRs are typically placed at checkpoints at intersections, on highways, or bridges and tunnels. As LPR information is aggregated, it can be used to triangulate location information on where individuals have traveled over time.

31 Request for Proposal [15F06720R0000063](#) (FBI, Redstone Arsenal Field Office, 2020).

32 Request for Proposal [15F06720R0000063](#), [Social Media Solicitation](#) (FBI, Redstone Arsenal Field Office, 2020).

33 Purchase Order [15F06721P0002431](#) (FBI, \$14.1 million, CMA Technology, Inc. 2021).

34 Sole Source Justification, [M0009619SUINS07](#) (Marine Corps Intelligence Surveillance Reconnaissance Enterprise, Thomson Reuters, 2019).

35 See, e.g., [Notice of Intent to Sole Source](#) (Marine Corps, Thomson Reuters, 2021).

ICE, for example, utilizes LPR data to conduct various forms of queries. ICE in a May 2021 Privacy Impact Assessment (PIA) acknowledged expanding its query abilities from full license plate numbers to allow for geofencing, partial license plates, and plate scanning applications on agent's mobile devices. In the PIA, ICE recognized the sensitivity and potential intrusiveness of such data, and explicitly acknowledged:

A “pattern of vehicle movement” can provide a sweeping account of location information and may disclose sensitive information about the vehicle based on the vehicle’s physical movements. For example, these queries can reveal excessive information outside the scope of an investigation, and could potentially indicate otherwise lawful activity, such as traveling to a doctor’s appointment, school, or participating in a First Amendment-protected activity (DHS, 2021, p. 6).

ICE states in the PIA that to mitigate this risk, personnel are “trained to focus on vehicles suspected to be involved in criminal activity” (DHS, 2021, p. 6). However, focusing on actual criminal suspects does not address the concern that such collection may in fact require a warrant; if the collection is gathering sufficient data to show a particular person’s pattern of movement, including such activities as participation in First Amendment-protected activities, this should require a warrant under the Supreme Court’s decision in *Carpenter*.

The most prominent national provider of LPR technology is Vigilant Solutions, which provides both stationary and mobile LPR systems manufactured by Motorola which apply optical character recognition (OCR) algorithms to identify plates. The ReaperHD Mobile License Plate Recognition Camera System is a vehicle-mounted box that can detect “hot listed” vehicles using real-time analytics (Motorola Solutions, n.d.). Vigilant has periodically contracted with federal agencies directly, such as a five-year, quarter-million dollar contract with DHS, or a small contract with a local FBI field office in Kailua Kona, Hawaii.³⁶

However, Vigilant data is most commonly utilized indirectly through Thomson Reuters CLEAR, which incorporates Vigilant’s database and contains over seven billion records and can provide hundreds of millions of sightings per month (Thomson Reuters, n.d.-b). For instance, a four-year, \$7.4 million dollar award between DHS and West Publishing Corporation, which is owned by Thomson Reuters, is described as being for “access to license plate reader database.”³⁷ The Department of Defense outlines why it sees particular value in CLEAR’s Vigilant database:

36 Purchase Order [HSBP1015P00498](#) (CBP, \$253.4k, Vigilant Solutions, LLC, 2015-2020); Purchase Order [15JA5418P00000346](#) (FBI, \$5.4k, Kailua Kona Field Office, Vigilant Solutions, LLC, 2018-2019).

37 Purchase Order [70CDCR18P00000017](#) (ICE, \$7.4 million, West Publishing Corporation, 2017-2021).

Agents and officers also require license plate recognition capability that will combine national data with nationwide Vigilant Solutions data. This will enable law enforcement to take vehicle-involved investigations to a more precise level even with partial data (i.e. partial plates, geographic landmarks, and vehicle associations). These combined capabilities will allow the agency to quickly build a full picture of a person of interest through finding contact and location information, identifying associations, making connections between individuals, activities, locations, and more with the most recent and relevant information updated frequently.³⁸

The terms of the CLEAR indicate that “[d]ue to the regulated or private nature of some data in our information products such as credit header data, motor vehicle data, driver license data and voter registration data, you may need to complete a credentialing process which will include certifying what your legally permissible use of the data will be” (Thomson Reuters, 2020). CLEAR’s contracts stipulate that “[a]ccess to LPR data via the gateway in CLEAR is limited to subscribers that have a legitimate law enforcement or investigative purpose and a permissible use under the U.S. Drivers Privacy Protection Act (18 U.S.C. §2721 et seq.).”³⁹ This language raises questions how a private entity verifies that users possess such a “legitimate law enforcement or investigative purpose,” and whether such a check is helpful at all to have. Moreover, the obligation should be on government agencies to ensure that they are complying with legal requirements, including requirements for search warrants or appropriate court orders.

In its solicitation for Computer Assisted Legal Research, the FBI outlines several of the criteria it wishes for LPR data to obtain.⁴⁰

38 Limited Source Justification for CLEAR [Subscriptions HQ0034-19-F-0013](#) (Department of Defense, Force Protection Agency, Thomson Reuters, 2018).

39 Thomson Reuters General Terms and Conditions, Version 2.1, attached to [Notice of Contract No. 200000000689](#) (State of Michigan, \$1.8 million, West Publishing Corporation, 2020-2023).

40 Solicitation 15JPSS19R00000013, pp. 24-32 et seq. (FBI, Computer Assisted Legal Research 5, 2018); [full document pages [1-50](#) / pages [51-104](#)].

C.9.4.1.8 Vehicle data	
Query	Results
Searchable by	Required but not limited to
<ul style="list-style-type: none"> - Name - Date of Birth - SSN - Address 	<ul style="list-style-type: none"> - Ownership - Historical LP read data - Past location mapping - Geo coordinates
	<ul style="list-style-type: none"> Geo-fencing capability; Additional vehicles with same owner and/or address; Insurance claim data; Lienholders; Rental Contact Information; Violations/Tickets; Partial plate query; Plate captures

Figure 4. Example of LPR data requested in one FBI solicitation. Source: Solicitation 15JPSS19R00000013, pp. 24-32 et seq. (FBI, Computer Assisted Legal Research 5, 2018); [full document pages [1-50](#) / pages [51-104](#)].

In 2020, CBP contracted with Thundercat Technology LLC for more than \$500,000, for analytics equipment across several cities including Miami, Tucson, and Spokane.⁴¹ Thundercat dubs itself a “value-added reseller” of technology (Thundercat Technology, 2021). DHS has also contracted other vendors for LPR management support.⁴²

////

D. Other types of brokered data

Many additional forms of data on individuals are collected by data brokers and sold to government agencies. Many of these categories may fall outside ECPA, and therefore go beyond the question of the ECPA loophole that has enabled federal agencies to gain commercial access to data that would require legal process to obtain directly. However, as described above, the broad language of the Supreme Court’s decision in *Carpenter* suggests that other categories of data that can reveal the “privacies of life” when collected at scale, may also require law enforcement to obtain a warrant. Therefore, it is useful to outline briefly several of these categories of data that present significant privacy implications and are worthy of consideration, and further research. Although this is not an exhaustive list of the types of data available from brokers that also implicate privacy concerns, the examples below are illustrative of the types of data that law enforcement and intelligence agencies have sought to purchase from data brokers that raise privacy concerns.

41 Delivery Order [HSHQDC13D00002-70B03C20F00001399](#) (CBP, \$199.1k, Thundercat Technology, LLC, 2020); Delivery Order [HSHQDC13D00002-70B03C20F00001210](#) (CBP, \$359.9k, Thundercat Technology, LLC, 2020).

42 In April 2021, CBP entered into a \$548k contract with Chevo Consulting LLC for “license plate reader program management support.” Purchase Order [GS00Q14OADS111-70B03C21F00000352](#) (CBP, \$548k, Chevo Consulting LLC, 2020-2021).

1. Utilities

Utilities data can be used to ascertain addresses; power contracts and usage can be used to infer how many people live at a residence or when individuals are not at home ([Electronic Privacy Information Center, 2021](#)). ICE utilizes data from various utilities in order to effectuate arrests and sometimes deportations ([Joseph, 2017](#); [Lamdan, 2019](#); [Mijente & Just Futures Law, 2021](#)). West's CLEAR product has been a source for utility records for law enforcement ([Mijente & Just Futures Law, 2021](#)) although it may lose access to this data as of December 2021 ([Harwell 2021](#)). Previously, Army Intelligence has indicated that where individuals are not easily traceable via "traditional sources," utility data may provide the "only current and accurate address and phone number data available," and that CLEAR "offers the most comprehensive utility locator information on the market."⁴³

2. Biometrics

Biometrics include the measurement and analysis of unique physical or behavioral characteristics of individuals for verification or identification purposes. Because of the unique identifiers they provide, biometrics have a variety of applications in authentication, including building access, device unlocking, or banking. Examples of biometrics include facial recognition, fingerprints, iris recognition, voice recognition, or behavioral metrics including keystroke dynamics and signature recognition. Biometrics are seeing increasing importance in investigations. However, the use of facial recognition and other biometric tools for law enforcement and immigration enforcement purposes raises a series of threats to privacy and civil rights, including a disproportionate impact on Black and Brown communities ([Franklin, 2021](#); [Nojeim, 2021](#)). The most prominent biometrics aggregator is Clearview AI, which scrapes various platforms for images, often in violation of terms of use (see generally [Ferguson, 2021](#)). ICE, for instance, contracted with Clearview in 2020 ([Hatmaker, 2020](#)).

3. Mobility data

Certain mobility services, which includes ride shares, scooters, and bikes implemented by many cities across the United States, include real-time geolocation tracking features. Some cities, including the District of Columbia and Los Angeles, have compelled mobility service providers to disclose location information reflecting the travels of customers including trip origins, destinations, routes taken, and time of travel. CDT has urged that data reporting in the city planning context be limited to aggregated data rather than individual trip-level data ([Nojeim & Azarmi, 2020](#)). Data brokers are emerging that focus on mobility data ([Matute et al., 2020](#)), though it is unclear the

The use of facial recognition and other biometric tools for law enforcement and immigration enforcement purposes raises a series of threats to privacy and civil rights, including a disproportionate impact on Black and Brown communities.

43 Sole Source Justification, [M0009619SUINS07](#) (Marine Corps Intelligence Surveillance Reconnaissance Enterprise, Thomson Reuters, 2019).

extent to which private data brokers currently obtain or have contracts for mobility data specifically with law enforcement or intelligence services. However, the National Association of City Transportation Officials already anticipates law enforcement demand for this data, having issued guidance for how to manage law enforcement requests, which suggests that commercial demands may be on the horizon as well ([NACTO & IMLA, 2019](#)). Mobility data – which can include real-time location data on individuals – contains a wealth of information regarding movement patterns, “raising a host of privacy issues” ([Azarmi, 2020](#)). Government should be required to obtain a warrant in order to access such data ([Nojeim & Jain, 2021](#)).



Recommendations

As this report describes, there is an extensive ecosystem of data brokers, whose customers include federal law enforcement and intelligence agencies. The data that such government agencies purchase commercially includes vast amounts of sensitive information, including location data and biometrics.

Data brokers operate in a largely unregulated market and government agencies have been able to exploit gaps in explicit statutory and constitutional prohibitions to evade otherwise applicable legal requirements. Congress intended to regulate the circumstances under which much of this information could be disclosed to the government, as demonstrated by the enactment of ECPA, described above. However, 35 years have passed since Congress passed ECPA, and as with so many aspects of that statute, it does not provide adequate safeguards to clearly cover the digital world that we live in today ([Calabrese, 2017](#)).⁴⁴ Similarly, the Supreme Court in *Carpenter v. United States* recognized the sensitivity of data that can reveal the “privacies of life” and held that the government must obtain a warrant in order to obtain certain types of sensitive information from private third parties. However, government agencies have interpreted the opinion narrowly.⁴⁵

As a result, government agencies have been able to purchase sensitive data from brokers in an end run around otherwise applicable legal requirements under ECPA and the Fourth Amendment. While this report focuses on federal law enforcement and intelligence agencies, the analysis, findings, and recommendations should apply to state and local government actors as well.

As noted above, the most urgent issue revealed by this report is the necessity of closing the loophole that allows federal agencies to commercially acquire data that agencies would otherwise require legal process to obtain directly from service providers. In addition, policymakers and companies can and should take a number of additional steps to address the threats to civil liberties posed by agencies’

⁴⁴ See also <https://digitaldueprocess.org> [perma.cc/5FY6-RF2C].

⁴⁵ A forthcoming law review article analyzes lower court decisions interpreting *Carpenter* and finds that courts have been most likely to extend the warrant requirement where the data sought is considered to be revealing and significant amounts of data are being collected ([Tokson, 2021](#)). The analysis does not include collection by intelligence agencies, since only law enforcement collection can be tested in court when challenged by criminal defendants.

practices of purchasing vast quantities of sensitive information from data brokers.

Therefore, CDT offers a series of recommendations for policymakers and private companies to address these concerns.

////

A. For Policymakers

1. Congress should pass the Fourth Amendment Is Not for Sale Act.

This legislation seeks to close the ECPA loophole that, as evidenced by this report, has enabled an entire lucrative industry around government contracts for data that the government should not access without appropriate legal process. As described above, ECPA requires different types of legal process depending on the particular type of data. These protections of ECPA lose meaning if they can be so easily sidestepped. Left unaddressed, the threat is that the practice and industry will only expand further. The Fourth Amendment Is Not for Sale Act will close this loophole by amending ECPA to extend its protections to any “intermediary service provider that delivers, stores, or processes communications” of a “covered person” under the Act. It would create a category of information that is “illegitimately obtained” to include records obtained from an ECS provider or an RCS provider in a manner that violates service agreements or is inconsistent with privacy policies, or to records obtained by deceit. The bill explicitly provides that “A law enforcement agency of a governmental entity and an element of the intelligence community may not obtain from a third party in exchange for anything of value a covered customer or subscriber record or any illegitimately obtained information” ([Fourth Amendment Is Not For Sale Act, 2021](#)). It is important to recognize that this legislation would not cover all types of sensitive data that government agencies purchase commercially, such as biometric information. Additional legislative and policy measures will be required to fully address the concerns outlined in this report.

2. Law enforcement and intelligence agencies should stop purchasing sensitive data at scale (or access to collections of data) that reveal the “privacies of life” under the Supreme Court’s analysis in Carpenter v. United States - or abide by Fourth Amendment standards before searching through any such data.

As described above, many types of data, when collected at scale, can provide an “intimate window into a person’s life,” with the result that people have a reasonable expectation of privacy in such information. This could extend beyond the data covered by ECPA -- and therefore beyond the scope of the Fourth Amendment Is Not for Sale Act. For example, biometric data, which may be held by companies that are not ECS or RCS providers under ECPA, can be especially sensitive and highly privacy invasive

if used to track an individual's movements ([Center on Privacy & Technology, 2019](#); [The Constitution Project's Task Force on Facial Recognition Surveillance & Jake Laperruque, 2019](#)). Moreover, categories of data such as utility records from smart meters may be highly revealing when aggregated with other data.⁴⁶

When law enforcement agencies seek to acquire such sensitive information and use it with regard to a particular individual, the Fourth Amendment's warrant requirement should apply. With regard to acquisition and use of such data by intelligence agencies, although the government has argued that there is a foreign intelligence exception to the warrant requirement, the Fourth Amendment nonetheless applies to acquisition of data about Americans. Thus, even if the warrant requirement is ultimately determined by the Supreme Court not to apply, as intelligence agencies acknowledge, acquisition of data about Americans must meet the Fourth Amendment's reasonableness standard. Under this standard, intelligence agencies should not be permitted to simply purchase sensitive types of data from data brokers without establishing robust safeguards for collection, use, sharing, and retention of this data.

3. Law enforcement and intelligence agencies should provide transparency regarding their procurement processes, including their purchases of data from data brokers.

Government agencies should provide transparency for their procurement processes in any procurement for data about individual Americans. Solicitations and procurement awards should contain meaningful descriptions of the types of data sought and acquired, and the use to which it will be put. As noted above, the Defense Intelligence Agency disclosed, in response to a congressional request, that it purchases commercially available location data aggregated from smartphones, and described how it uses that data. Any federal law enforcement or intelligence agency that purchases data about Americans should publicly disclose the types of data that it purchases and the ways in which it uses that data. Agencies should update such public disclosures on a regular periodic basis. In addition, agency Privacy and Civil Liberties Officers should ensure that Privacy Impact Assessments are prepared and released before their agency obtains access to data about Americans held in a commercial database, and that the privacy and civil liberties risks attendant to agency access to such data are properly described in the PIA.⁴⁷

46 The U.S. Court of Appeals for the Fourth Circuit recently held in *Leaders of a Beautiful Struggle v. Baltimore Police Department* that the police department's warrantless collection of location information through aerial surveillance, when combined with other data, violated individuals' expectation of privacy under *Carpenter* and required a warrant ([Li & Nojeim, 2021](#)).

47 For example, the form the Department of Homeland Security uses to guide the creation of PIAs requires the person preparing the report to explain why the project at issue uses information obtained from commercial sources and how that information will be used. Department of Homeland Security, Privacy PIA Template, p. 3 Section 2.3, available at <https://www.dhs.gov/xlibrary/assets/privacy/>

4. Congress should conduct hearings to examine data broker sales to foreign governments, as well as U.S. intelligence agencies' sharing of data purchased from data brokers.

Congress should explore the extent to which data brokers currently sell sensitive information regarding Americans to foreign governments. This will enable Congress to assess whether and to what extent limits on intelligence agency purchases of such data should be accompanied by limits on the ability of data brokers to sell information to foreign governments. In addition, Congress should examine U.S. intelligence agencies practices regarding the sharing of sensitive information about Americans purchased from data brokers with foreign governments.

5. Congress should enact comprehensive consumer privacy legislation.

In addition to restricting the ability of law enforcement and intelligence agencies to purchase information from data brokers, Congress should also protect the rights of consumers whose information is collected and sold by brokers, which includes sales in other contexts. The time is overdue for comprehensive consumer privacy legislation, including regulation of data brokers, and limits on what personal data companies are able to sell, as well as safeguards for when personal data is sold. As CDT has previously proposed, this should include such measures as encouraging the Federal Trade Commission to create an opt-out registry of data brokers. A federal consumer privacy law should also limit the data that brokers can collect, process, and share, and provide consumers with the ability to understand what information data brokers have collected about them and with a meaningful ability to have the information deleted, obscured or corrected.

6. Congress should increase funding for the Federal Trade Commission to enforce consumer privacy rules, including regulations of data brokers.

As CDT has urged previously, Congress should increase funding for the Federal Trade Commission to enforce rules protecting consumer privacy. This should include additional resources to enable the Commission to regulate and enforce restrictions governing data brokers.

7. GAO should conduct a study to assess expenditures on data from data brokers.

GAO should examine expenditures by federal law enforcement and intelligence agencies on obtaining sensitive data about Americans from data brokers. The GAO

study can build on their previous work on data brokers ([GAO, 2013](#)) and should include calculating the total dollar amount spent by such agencies on such data from data brokers in the most recent calendar year.

8. Federal law enforcement and intelligence agencies that purchase data from data brokers should implement regular independent audits to assess reliability and efficacy and to prevent discrimination.

To the extent that implementation of the recommendations above does not eliminate federal law enforcement and intelligence agency purchases of information from data brokers, such agencies should take further steps to mitigate the risks posed by such purchases of sensitive data. In particular, any federal law enforcement or intelligence agency that purchases data about Americans from data brokers should adopt a program for regular independent audits to assess the agency's use of such data. The audits should measure the reliability of the data and whether the agency's use of such data is effective in achieving the agency's purposes. The agencies should also implement regular independent audits to assess whether use of the data sets results in discrimination against any protected classes or a disparate impact on such groups. If the results of any audits reflect unreliability, ineffectiveness or discrimination, the agency should modify or discontinue its use of such sensitive data to address the issue.

9. Federal law enforcement should provide notice to criminal defendants of use of data from data brokers.

In many contexts, the law requires federal law enforcement to provide notice to criminal defendants that evidence to be introduced against them has been obtained through certain means – such as through surveillance under the Foreign Intelligence Surveillance Act – to enable defendants to challenge the legality of such evidence. Given this report's findings that law enforcement agencies often obtain sensitive data from data brokers in an end run around otherwise applicable legal requirements under ECPA and the Fourth Amendment, federal law enforcement agencies should provide notice to criminal defendants whenever the government intends to use data purchased from data brokers against a criminal defendant in any court proceeding.

////

B. For Private Companies

1. Companies that are covered by ECPA should take steps to prevent the sale of their data downstream to exploit the ECPA loophole.

In the absence of legislation that would close the ECPA loophole described in this report, ECS and RCS providers covered by ECPA should use contractual clauses

whenever they sell data to a non-covered entity to prohibit the further sale of that data to law enforcement absent appropriate legal process under ECPA.

2. Companies covered by ECPA should include information about sales of data in their transparency reports.

Numerous companies covered by ECPA as ECS and RCS providers publish regular transparency reports providing statistical and other information regarding the requests they receive from governments seeking access to their customers' data. Companies should expand these transparency reports to include information regarding their sales of data to data brokers. The reporting should also include statistical information describing any sales of data outside the United States, including to foreign governments.

3. Data brokers should issue regular transparency reports.

Data brokers should be more transparent about their sales to law enforcement and intelligence agencies of sensitive consumer information, and access to databases containing such information. Many communication service providers already issue transparency reports⁴⁸ that describe to the public the number of disclosures to law enforcement and intelligence agencies that they make; data brokers should make similar disclosures regarding law enforcement sales. Data brokers' reports would be structured somewhat differently and would need to include the type and number of commercial transactions they have engaged in with government purchasers, as well as the type and quantity of data disclosed.



48 See for example https://www.t-mobile.com/news/_admin/uploads/2021/07/2020-Transparency-Report.pdf [perma.cc/9RYM-MLTL]

Annex - Methods, Challenges, and Tactics for Further Research

For purposes of this report, we used a variety of methods to identify relevant government Requests for Proposals (RFPs). These included searches of awards as well as government documents on a variety of contract-compilation services. Govtribe is the most comprehensive and user-friendly, though other databases such as USASpending and SAMS were also consulted. We restricted searches to relevant agencies and divisions, and gave priority to documents issued after the Supreme Court's decision in *Carpenter v. United States* in 2018. We referenced keywords from a combination of awards, government documents, news articles, and agency memoranda to attempt to pinpoint alternative ways that activities were described. In total we collected approximately 150 documents. Through our review, we found that about 50 documents contained sufficient information to be referenced in this report. Unfortunately, the majority of documents lacked clarity on the specific nature of the contract in question, although they appeared to cover transactions involving personal data.

Indeed, this lack of transparency leads to one of the greatest challenges in studying data broker relationships with law enforcement and intelligence agencies. Potentially due to rising public scrutiny, it appears that by design data, broker relationships are not intended to be unraveled. They are highly attenuated, and contracts are shrouded in secrecy and often contain strict non-disclosure provisions. For example, one Babel Street contract addendum contains numerous provisions preventing disclosure of Locate X, preventing it from being “used as the basis for any legal process in any country, including as the basis for a warrant, subpoena, or any other legal or administrative action” ([Babel Street, 2020a, p. 9](#)). These prohibitions would appear to go beyond what would be necessary to protect ordinary business interests or trade secrets.

On the other hand, one factor assisting our research is that, since the market for data is a commercial industry, companies do seek to maintain branding and marketing of their products, an objective at some tension with preserving their secrecy. As a result, data broker marketing materials or communications may be more transparent in disclosing the capabilities of their databases and services. This is perhaps one reason some organizations have had success in obtaining broker relationship documents through freedom of information requests. As law enforcement databases are often contracted locally or at county and state levels, there may be value in submitting requests at the local level as well. In making freedom of information requests, it is important to become familiar with the terminology and designations utilized by

agencies in referencing data broker programs. For example, the Justice Department maintains a designation for Computer Assisted Legal Research 5 (CALR 5) and entered into a \$12.7 million contract with West Publishing Co. in 2020 with just the description ‘CALR 5.’⁴⁹ While the phrase ‘legal research’ may appear at first glance to involve research of legal resources such as cases, statutes, and sources to be cited in legal documents, the actual scope of what the DOJ, particularly the FBI, consider to fall under CALR 5 is vastly broader. Procurement contracts and solicitations typically provide little transparency as to their actual purposes or details on their terms.



⁴⁹ Delivery Order [15JPSS19D00000122-15JPSS20F00001100](#) (DOJ, \$12.7 million, West Publishing Corporation, 2020-2021).

References

- Affidavit, In the Matter of the Search of Information Regarding Accounts Associated with Certain Location and Date Information, Maintained on Computer Servers Controlled by Google, Inc., 1:18-mj.169 (W.D. Tex., Mar. 14, (2018).*
- Aftergood, S. (2021, October 4). A Push to Elevate Open Source Intelligence. Federation Of American Scientists. <https://fas.org/blogs/secretcy/2021/10/open-source-elevate/> [https://perma.cc/G8D3-ESQD]
- Assembly Bill No. 1202, § 1798.99.80 et seq. Cal. Civ. Code (2019). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202 [https://perma.cc/U6DE-QE9R]
- Azarmi, M. (2020). *Smart-Enough Cities: Governments That Seek Mobility Data Must Respect Individual Privacy*. Center for Democracy & Technology. <https://cdt.org/insights/report-smart-enough-cities-governments-that-seek-mobility-data-must-respect-individual-privacy/> [https://perma.cc/FB47-4GMW]
- Babel Street. (2020a). *End User Subscription Terms International Locate X Addendum*. Babel Street. <https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/712032/750265271566952-terms-and-conditions-2020-07-20-1423.pdf> [https://perma.cc/54S2-ZBNS]
- Babel Street. (2020b). *Service definition document, Locate X*. Babel Street. <https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/712032/750265271566952-service-definition-document-2020-07-20-1357.pdf> [https://perma.cc/XU7Z-NRDA]
- Babel Street. (2021a). *Criminal Investigations*. Babel Street. <https://babelstreet.com/government/criminal-investigations> [https://perma.cc/687W-ZQ6G]
- Babel Street. (2021b, July 16). *Privacy Policy*. Babel Street. <https://www.babelstreet.com/privacy-policy> [https://perma.cc/5N9X-P7DR]
- Barbaricum. (2021). *About*. Barbaricum. <https://barbaricum.com/about/> [https://perma.cc/YAT9-FG8E]
- Biddle, S. (2021, November 4). The U.S. Treasury Is Buying Private App Data to Target and Investigate People. *The Intercept*. <https://theintercept.com/2021/11/04/treasury-surveillance-location-data-babel-street/> [https://perma.cc/VEV8-U3M3]
- Brennan Center for Justice. (2019). *Statement of Civil Rights Concerns About Monitoring of Social Media by Law Enforcement*. Brennan Center for Justice. <https://www.brennancenter.org/sites/default/files/2019-11/Social%20media%20monitoring%20statement.pdf> [https://perma.cc/5SHM-SBG8]
- Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (ECF No. 29), United States v. Chatric No. 3:19-CR-00130 (E.D. Va.). (2019).*
- Calabrese, C. (2017, July 27). Broad Support for the ECPA Modernization Act. *Center for Democracy and Technology*. <https://cdt.org/insights/broad-support-for-the-ecpa-modernization-act/> [https://perma.cc/88CN-YGZJ]
- Carpenter v. United States*, 138 S. Ct. 2206 (2018).
- CBS News. (2020, February 5). *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*. CBS News. <https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/> [https://perma.cc/T95Y-W5SX]

- Center on Privacy & Technology. (2019). *America Under Watch: Face Surveillance in the United States*. Georgetown University. <https://www.americaunderwatch.com> [https://perma.cc/9T8S-8RQU]
- CIA. (2017). *CIA Procedures Approved by the Attorney General Pursuant to Executive Order 12333*. Central Intelligence Agency. <https://www.cia.gov/static/54871453e089a4bd7cb144ec615312a3/CIA-AG-Guidelines-Signed.pdf> [https://perma.cc/F2RQ-VN]6]
- Cox, J. (2020, August 25). Customs and Border Protection Paid \$476,000 to a Location Data Firm in New Deal. *Vice*. <https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs> [https://perma.cc/9B82-KKCB]
- Cox, J. (2021a, January 11). Leaked Location Data Shows Another Muslim Prayer App Tracking Users. *Vice*. <https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first> [https://perma.cc/42RQ-PL2G]
- Cox, J. (2021b, March 4). Military Unit That Conducts Drone Strikes Bought Location Data From Ordinary Apps. *Vice*. <https://www.vice.com/en/article/y3g97x/location-data-apps-drone-strikes-iowa-national-guard> [https://perma.cc/CD8N-24KY]
- Cox, J. (2021c, March 10). Florida Prison System Bought Location Data from Apps. *Vice*. <https://www.vice.com/en/article/3an9jy/florida-prison-locate-x-location-data-department-of-corrections> [https://perma.cc/6Y2X-Y4FL]
- Dang, S., & Kerber, R. (2021, June 9). Thomson Reuters shareholder support for human rights review rises. *Reuters*. <https://www.reuters.com/business/thomson-reuters-shareholder-support-human-rights-review-rises-2021-06-09/> [https://perma.cc/R99Y-MRV7]
- de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, 3(1), 1376. <https://doi.org/10.1038/srep01376>
- Defense Intelligence Agency. (2021). *Defense Intelligence Agency Memo, U-21-0002/OCC-1, Clarification of information Briefed During DIA's 1 December Briefing on CTD*. Defense Intelligence Agency. <https://int.nyt.com/data/documenttools/dia-memo-for-wyden-on-commercially-available-smartphone-locational-data/d7d41dccdd1d46b0/full.pdf> [https://perma.cc/VDN5-VRAR]
- Delaney, C., & Beck, J. (2014). *Intelligence-Led Policing with the ArcGIS Platform*. <http://leiu.org/training/event/speaker/2014/chris-delaney> [https://perma.cc/HZA4-XFAP]
- Department of Defense. (2016). *Department of Defense Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities*. Department of Defense. <https://dodcio.defense.gov/Portals/46/DoDM%20%205240.01.pdf> [https://perma.cc/NA3P-J9FU]
- DHS. (2021). *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader (LPR) Data from a Commercial Service*. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/privacy-pia30b-ice-acquisitionanduseoflprdatafromacommercialservice-june2021_0.pdf [https://perma.cc/YX6T-TEUY]
- Electronic Privacy Information Center. (2021). *EPIC - The Smart Grid and Privacy*. <https://archive.epic.org/privacy/smartgrid/smartgrid.html> [https://perma.cc/QFZ6-EKTF]
- ESRI. (2017). *GIS for Crime Analysis*. Environmental Systems Research Institute. <https://www.esri.com/~media/Files/Pdfs/library/brochures/pdfs/gis-for-crime-analysis.pdf> [https://perma.cc/HQH5-U2VB]
- Exec. Order No. 12333* (Section 2.3(a)). (1981).
- Factual. (2019, January 17). MMA Report: Use Cases for Location Data Beyond Geo-fencing. *Factual*. <https://www.factual.com/blog/mma-report-use-cases-for-location-data-beyond-geo-fencing/> [https://perma.cc/7AWS-YMUY]

- Fang, L. (2020, June 24). FBI Expands Ability to Collect Cellphone Location Data, Monitor Social Media, Recent Contracts Show. *The Intercept*. <https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/> [<https://perma.cc/Y2DN-RVGW>]
- Federal Trade Commission. (2012). *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*. Federal Trade Commission. <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> [<https://perma.cc/8UUD-2NF7>]
- Federal Trade Commission. (2014). *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014)*. Federal Trade Commission. <https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014> [<https://perma.cc/XU7X-QGKA>]
- Federal Trade Commission. (2021). *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*. Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf [<https://perma.cc/4SG8-UHNN>]
- Ferguson, A. G. (2019). *The Rise of Big Data Policing*. NYU Press.
- Ferguson, A. G. (2021). Facial Recognition and the Fourth Amendment. *Minnesota Law Review*, 105, 1105.
- Forbrukerrådet. (2020). *OUT OF CONTROL How consumers are exploited by the online advertising industry*. Forbrukerrådet. <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf> [<https://perma.cc/EJ7K-LSFX>]
- Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong (2021).
- Franklin, S. B. (2018, July 25). Carpenter and the End of Bulk Surveillance of Americans. *Lawfare*. <https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans> [<https://perma.cc/6H39-VQQB>]
- Franklin, S. B. (2021, October 14). *Recognizing the Threats: Congress Must Impose a Moratorium on Law Enforcement Use of Facial Recognition Tech*. Center for Democracy and Technology. <https://cdt.org/insights/recognizing-the-threats-congress-must-impose-a-moratorium-on-law-enforcement-use-of-facial-recognition-tech> [<https://perma.cc/R25G-XCML>]
- Future of Privacy Forum. (2016). *Smart Places*. <https://www.smart-places.org/> [<https://perma.cc/E5XC-K42N>]
- GAO. (2013). *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*. United States Government Accountability Office. <https://www.gao.gov/assets/gao-13-663.pdf> [<https://perma.cc/5CCA-WWQL>]
- German, M., & Hockett, E. (2017, May 2). *Standards for Opening an FBI Investigation So Low They Make the Statistic Meaningless | Brennan Center for Justice*. <https://www.brennancenter.org/our-work/analysis-opinion/standards-opening-fbi-investigation-so-low-they-make-statistic> [<https://perma.cc/MT69-RU6F>]
- Giant Oak Inc. (2019, November 26). *Giant Oak Privacy Policy*. [https://cdn2.hubspot.net/hubfs/3396037/Giant%20Oak%20website%20privacy%20policy%201.3.20%20\(Final\).pdf](https://cdn2.hubspot.net/hubfs/3396037/Giant%20Oak%20website%20privacy%20policy%201.3.20%20(Final).pdf) [<https://perma.cc/2G93-JLLT>]
- Grand Jury Action No. 21-20 (BAH)*, (D.D.C. July 16, 2021).
- Grundy, Q., Chiu, K., Held, F., Continella, A., Bero, L., & Holz, R. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: Traffic, content, and network analysis. In *BMJ* (Vol. 364, p. 1920).
- Harwell, D. (2021). Utility giants agree to no longer allow sensitive records to be shared with ICE. *Washington Post*. <https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/> [<https://perma.cc/MXU2-QQHR>]

- Hatmaker, T. (2020, August 14). Clearview AI landed a new facial recognition contract with ICE. *TechCrunch*. <https://techcrunch.com/2020/08/14/clearview-ai-ice-hsi-contract-2020/> [<https://perma.cc/5PPD-2DJU>]
- Horwitz, J., & Olson, P. (2020, September 29). Twitter Partner's Alerts Highlight Divide Over Surveillance. *Wall Street Journal*. <https://www.wsj.com/articles/twitter-partners-alerts-highlight-divide-over-surveillance-11601417319> [<https://perma.cc/N8Q3-KA5B>]
- Joseph, G. (2017, May 12). Where ICE Already Has Direct Lines To Law-Enforcement Databases With Immigrant Data. *NPR*. <https://www.npr.org/sections/codeswitch/2017/05/12/479070535/where-ice-already-has-direct-lines-to-law-enforcement-databases-with-immigrant-d> [<https://perma.cc/D8M8-CVGE>]
- Kalat, D. (2019, October 17). How Outdated Privacy Laws Might Affect You And Your Data. *Strategic Business Consulting News and Analysis from BRG | ThinkSet*. <https://thinksetmag.com/insights/kalat-computer-laws> [<https://perma.cc/TR6T-LQYM>]
- Katz v. United States*, 389 U.S. 347 (1967).
- Keegan, J., & Ng, A. (2021, September 30). There's a Multibillion-Dollar Market for Your Phone's Location Data. *The Markup*. <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data> [<https://perma.cc/NES5-HKEG>]
- Kris, D. (2017, March 21). The CIA's New Guidelines Governing Publicly Available Information. *Lawfare*. <https://www.lawfareblog.com/cias-new-guidelines-governing-publicly-available-information> [<https://perma.cc/K78Z-6K96>]
- Lamdan, S. (2019). When Westlaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing. *N.Y.U. Review of Law & Social Change*, 43(2), 255–293.
- Lazarus, D. (2019, November 5). Shadowy data brokers make the most of their invisibility cloak. *Los Angeles Times*. <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> [<https://perma.cc/NP2H-LF7Q>]
- Levinson, C. (2020, March 5). Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones. *Protocol — The People, Power and Politics of Tech*. <https://www.protocol.com/government-buying-location-data> [<https://perma.cc/86X8-8VRQ>]
- LexisNexis. (2021a). *ThreatMetrix® for Government*. LexisNexis Risk Solutions. <https://risk.lexisnexis.com/products/threatmetrix-for-government> [<https://perma.cc/KJ3C-YMYL>]
- LexisNexis. (2021b). *ThreatMetrix—Cybersecurity Risk Management*. LexisNexis Risk Solutions. https://risk.lexisnexis.com/-/media/files/product%20pages/brochure/lhrs-threatmetrix_brochure-nxr14716-00-1120-en-us.pdf (PDF download) [<https://perma.cc/7X3N-6PY7>]
- Li, E., & Nojeim, G. (2021, July 19). *Court Rules that Warrantless Persistent Aerial Surveillance Is Unconstitutional*. Center for Democracy and Technology. <https://cdt.org/insights/court-rules-that-warrantless-persistent-aerial-surveillance-is-unconstitutional/> [<https://perma.cc/N989-CQUK>]
- Martin, K. (2015). Ethical Issues in the Big Data Industry. *MIS Quarterly Executive*, 14(2). <https://aisel.aisnet.org/misqe/vol14/iss2/4> [<https://perma.cc/49K8-L22P>]
- Matute, J., Cohen-D'Agostino, M., & Brown, A. (2020). *Sharing Mobility Data for Planning and Policy Research*. UC Office of the President: University of California Institute of Transportation Studies. <https://escholarship.org/uc/item/88p873g4> [<https://perma.cc/78VZ-UCTP>]


- Mijente [@ConMijente]. (2020, July 23). *Dataminr is a massive data broker (they claim to mine 10,000 public data sets)*. Twitter. <https://twitter.com/ConMijente/status/1286363830654627840> [<https://perma.cc/46MW-HPGF>]
- Mijente & Just Futures Law. (2021). *The Data Broker to Deportation Pipeline: How Thomson Reuters & LexisNexis Share Utility & Commercial Data with ICE*. Mijente and Just Futures Law. <https://www.flipsnack.com/JustFutures/commercial-and-utility-data-report/full-view.html> [<https://perma.cc/G7H3-HGKT>]
- Motorola Solutions. (n.d.). *Mobile License Plate Recognition—Motorola Solutions*. Retrieved November 8, 2021, from https://www.motorolasolutions.com/en_us/video-security-analytics/license-plate-recognition-camera-systems/reaperhd-mobile-lpr-system.html [<https://perma.cc/7CG9-APMX>]
- NACTO & IMLA. (2019). *Managing Mobility Data*. National Association of City Transportation Officials and International Municipal Lawyers Association. https://nacto.org/wp-content/uploads/2019/05/NACTO_IMLA_Managing-Mobility-Data.pdf [<https://perma.cc/36D3-XWLX>]
- Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
- Nojeim, G. (2021, June 3). *CDT Joins OTI, Upturn, and the Leadership Conference for Civil and Human Rights in Call for Moratorium on Law Enforcement Use of Facial Recognition*. Center for Democracy and Technology. <https://cdt.org/insights/cdt-joins-oti-upturn-and-the-leadership-conference-for-civil-and-human-rights-in-call-for-moratorium-on-law-enforcement-use-of-facial-recognition/> [<https://perma.cc/VPC9-C27Y>]
- Nojeim, G., & Azarmi, M. (2020, March 20). *CDT's Letter to the District DOT Regarding Mobility Data*. Center for Democracy and Technology. <https://cdt.org/insights/cdts-letter-to-the-district-dot-regarding-mobility-data/> [<https://perma.cc/T3KW-AH7P>]
- Nojeim, G., & Jain, S. (2021, August 23). *CDT and EPIC File Amicus Brief Arguing for Protections for E-Scooter Location Information*. Center for Democracy and Technology. <https://cdt.org/insights/cdt-and-epic-file-amicus-brief-arguing-for-protections-for-e-scooter-location-information/> [<https://perma.cc/N4G5-U4X6>]
- Note. (2021). Geofence Warrants and the Fourth Amendment. *Harv. L. Rev.*, 134(7), 2508.
- Office of the Director of National Intelligence. (2020). *Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive Order 12333*. Office of the Director of National Intelligence. https://www.intel.gov/assets/documents/702%20Documents/declassified/AGGs/ODNI%20guidelines%20as%20approved%20by%20AG%2012.23.20_OCR.pdf [<https://perma.cc/Z5YN-2NSA>]
- Palantir. (2021). *About | Palantir*. <https://www.palantir.com/about/> [<https://perma.cc/857Q-4B9S>]
- Perez, S., & Whittaker, Z. (2020, October 1). Facebook sues two companies engaged in data scraping operations. *TechCrunch*. <https://techcrunch.com/2020/10/01/facebook-sues-two-companies-engaged-in-data-scraping-operations/> [<https://perma.cc/KM89-3NLW>]
- Protection Of Personal Information, 9 V.S.A. § 2430(4)(A) (2019). <https://legislature.vermont.gov/statutes/section/09/062/02430> [<https://perma.cc/ER2J-5DZG>]
- Rieke, A., Yu, H., Robinson, D., & Van Hoboken, J. (2016). *Data brokers in an open society*. Open Society Foundations. <https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf> [<https://perma.cc/B2RZ-JH48>]
- Savage, C. (2021, January 22). Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says. *The New York Times*. <https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html> [<https://perma.cc/GX5V-RNXY>]


- Sherman, J. (2021a). *Data Brokers and Sensitive Data on U.S. Individuals*. Duke University. <https://sites.sanford.duke.edu/techpolicy/report-data-brokers-and-sensitive-data-on-u-s-individuals/> [<https://perma.cc/KJV6-MVJA>]
- Sherman, J. (2021b, April 8). Federal Privacy Rules Must Get “Data Broker” Definitions Right. *Lawfare*. <https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right> [<https://perma.cc/L8SQ-7L7A>]
- Skyhook. (2021, February 1). *Services Privacy Policy*. <https://www.skyhook.com/privacy-services> [<https://perma.cc/CFD4-EW5L>]
- Tau, B. (2020, June 19). IRS Used Cellphone Location Data to Try to Find Suspects. *Wall Street Journal*. <https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815> [<https://perma.cc/W9YT-HWL2>]
- Tau, B. (2021a, February 22). Treasury Watchdog Warns of Government’s Use of Cellphone Data Without Warrants. *Wall Street Journal*. <https://www.wsj.com/articles/treasury-watchdog-warns-of-governments-use-of-cellphone-data-without-warrants-11614003868> [<https://perma.cc/4KBF-ZHZV>]
- Tau, B. (2021b, September 15). Law Enforcement’s Use of Commercial Phone Data Stirs Surveillance Fight. *Wall Street Journal*. <https://www.wsj.com/articles/law-enforcements-use-of-commercial-phone-data-stirs-surveillance-fight-11631707201> [<https://perma.cc/D7ZG-TCLP>]
- Tau, B. (2021c, November 18). How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies. *Wall Street Journal*. <https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202> [<https://perma.cc/7QZT-2QMY>]
- The Constitution Project’s Task Force on Facial Recognition Surveillance & Jake Laperruque. (2019). *Facing the Future of Surveillance*. <https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/> [<https://perma.cc/FM68-XTTN>]
- Thomson Reuters. (n.d.-a). *Government solutions*. Retrieved November 8, 2021, from <https://www.thomsonreuters.com/en/products-services/government.html> [<https://perma.cc/JTX8-P6CZ>]
- Thomson Reuters. (n.d.-b). *Law Enforcement Solutions | CLEAR*. Retrieved November 8, 2021, from <https://legal.thomsonreuters.com/en/products/clear-investigation-software/law-enforcement> [<https://perma.cc/H2RE-TWLP>]
- Thomson Reuters. (2019, October 28). *Thomson Reuters to provide US DOJ, FBI with legal and investigative tools under new multi-year contract*. <https://www.thomsonreuters.com/en/press-releases/2019/october/thomson-reuters-to-provide-us-doj-fbi-with-legal-and-investigative-tools-under-new-multi-year-contract.html> [<https://perma.cc/89RJ-WG2N>]
- Thomson Reuters. (2020). *CLEAR, Federal Supply Schedule (2020-2021)*. Thomson Reuters. https://www.gsaadvantage.gov/ref_text/GS02F026DA/GS02F026DA_online.htm [<https://perma.cc/83NR-4V GK>]
- Thomson Reuters. (2021). *Thomson Reuters Annual Report 2020*. Thomson Reuters. <https://ir.thomsonreuters.com/financial-information/annual-reports> [<https://perma.cc/PK5U-WHY Y>]
- Thundercat Technology. (2021). *Thundercat Technology*. <https://www.thundercattech.com/> [<https://perma.cc/W35G-LCWP>]
- T-Mobile. (2018, June 15). *T-Mobile Ltr to Sen. Wyden*. <https://www.wyden.senate.gov/imo/media/doc/T%20Mobile%206-15-18%20Ltr%20to%20Sen.%20Wyden.pdf> [<https://perma.cc/9T4R-8CCF>]
- Tokson, M. (2021). The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021. *Harvard Law Review, Forthcoming University of Utah College of Law Research Paper No. 470*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3932015 [<https://perma.cc/22J6-ZCQ9>]

- Toonders, J. (2014, July 23). Data Is the New Oil of the Digital Economy. *Wired*. <https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> [<https://perma.cc/T8XK-ERPL>]
- United States for PRTT Order for One Whatsapp Chief Account for Investigation of Violation of 21 U.S.C. § 841*, 2018 WL 1358812 (D.D.C. March 2, 2018).
- United States v. Jones*, 132 S. Ct. 945. (2012).
- United States v. Perretta*, No. 1:21-mj-490 (D.D.C. July 12, 2021).
- United States v. Warshak*, 631 F.3d 266 (6th Cir 2010).
- US Senate Committee On Commerce, Science, and Transportation. (2013). *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. US Senate Committee On Commerce, Science, and Transportation. <https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577> [<https://perma.cc/3QPC-NN9R>]
- Venntel. (2021, September). *Venntel Privacy Policy*. <https://www.venntel.com/privacy-policy> [<https://perma.cc/R6TS-22CF>]
- Warren, Maloney, Wyden, DeSaulnier Probe Data Broker's Collection of Data on Black Lives Matter Demonstrators. (2020, August 4). House Committee on Oversight and Reform. <https://oversight.house.gov/news/press-releases/warren-maloney-wyden-desaulnier-probe-data-brokers-collection-of-data-on-black> [<https://perma.cc/VW5N-QV4W>]
- Williams, R. (2019, August 29). Study: Most location-based ad spending is wasted on bad targeting. *Marketing Dive*. <https://www.marketingdive.com/news/study-most-location-based-ad-spending-is-wasted-on-bad-targeting/561908> [<https://perma.cc/534Q-EW8R>]
- Wyden, R. (2021, April 21). *S.1265 - 117th Congress (2021-2022): Fourth Amendment Is Not For Sale Act (2021/2022)* [Legislation]. <https://www.congress.gov/bill/117th-congress/senate-bill/1265> [<https://perma.cc/KG4V-J5S8>]
- ZeroFox. (2020, July 20). *Privacy Policy*. ZeroFox. <https://www.zerofox.com/privacy-policy/> [<https://perma.cc/848E-7XAM>]
- ZeroFox. (2021). *Digital Risk Protection and Management Platform*. ZeroFox. <https://www.zerofox.com/platform/> [<https://perma.cc/6R8G-ERCL>]

 cdt.org

 cdt.org/contact

 Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

 202-637-9800

 @CenDemTech

