UNIVERSITY OF PITTSBURGH LAW REVIEW ONLINE
Vol. 84 ● 2023

WHERE THE FOURTH AMENDMENT FAILS: USING THE EUROPEAN COURT OF HUMAN RIGHTS FRAMEWORK TO LIMIT LAW ENFORCEMENT AGENCIES' PURCHASES OF PEOPLE'S DATA FROM DATA BROKERS

Zev T. Chabus

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

WHERE THE FOURTH AMENDMENT FAILS: USING THE EUROPEAN COURT OF HUMAN RIGHTS FRAMEWORK TO LIMIT LAW ENFORCEMENT AGENCIES' PURCHASES OF PEOPLE'S DATA FROM DATA BROKERS

Zev T. Chabus[*]

The Fourth Amendment serves a vital purpose in American jurisprudence: it protects the public from unreasonable searches and seizures by the government. However, the Fourth Amendment has a glaring loophole: government entities can obtain people's private data, without a search warrant, simply by buying such data from third parties. The Supreme Court has not definitively addressed this issue. However, the European Court of Human Rights has produced a workable framework that, if implemented by Congress and applied by the courts, would protect people's data from being used by law enforcement agencies without a search warrant. This Article discusses the third parties—data brokers—that sell data to law enforcement agencies and explores how the ECtHR framework can prevent such use.

[*] B.A., Queens College, City University of New York, 2017; J.D., Cornell Law School, 2022. Thank you to the staff of the *University of Pittsburgh Law Review* for their work on this Article, as well as Sarah St. Vincent for providing insight into different legal frameworks regarding privacy issues.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

Table of Contents

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

INTRODUCTION

When people shop online, companies are tracking them to see what they look at and what, if anything, they buy.[1] When someone uses a credit card in a supermarket, the credit card company and the supermarket know that person's food preferences.[2] People's cell phones track their locations, and their phone service provider knows where they are.[3] These companies then sell this information to third parties,[4] some of whom then sell the information to law enforcement.[5]

These third parties, known as data brokers, compile extensive dossiers on each person whose information they have acquired.[6] And while law enforcement agencies generally need to obtain a search warrant before searching for someone's private information,[7] they can currently get around this requirement by purchasing the information from data brokers instead.[8]

Accordingly, there are holes in the Unites States' requirement for a search warrant—it seemingly does not apply when law enforcement agencies purchase data

[1] *See* Zach Whittaker, *Oracle's BlueKai Tracks You Across the Web. That Data Spilled Online*, TECHCRUNCH (June 19, 2020, 10:30 AM), https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ [https://perma.cc/VZ4E-YE9L].

[2] *See* Burt Helm, *Credit Card Companies Are Tracking Shoppers Like Never Before: Inside the Next Phase of Surveillance Capitalism*, FAST CO. (May 12, 2020), https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism [https://perma.cc/MD84-UDW9].

[3] Rob Pegoraro, *Apple and Google Remind You About Location Privacy, But Don't Forget About Your Wireless Carrier*, USA TODAY (Nov. 23, 2019, 6:00 AM), https://www.usatoday.com/story/tech/columnist/2019/11/23/location-data-how-much-do-wireless-carriers-keep/4257759002/ [https://perma.cc/VGV5-ZPW4].

[4] *See* Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html [https://perma.cc/ELB5-8J2U].

[5] *See* Sara Morrison, *Here's How Police Can Get Your Data—Even if You Aren't Suspected of a Crime*, VOX (July 31, 2021, 9:00 AM), https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant [https://perma.cc/589T-YPQ9].

[6] *See* Singer, *supra* note 4.

[7] Katz v. United States, 389 U.S. 347, 357 (1967).

[8] Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020, 7:30 AM), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 [https://perma.cc/AT7K-9PFE].

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

from third parties, such as data brokers, and to the information they provide.[9] However, law enforcement agencies use information provided by data brokers even when the agencies are not actively conducting any investigations.[10] As such, there should be a different framework to evaluate when law enforcement agencies should have access to this information, even when it is provided by third parties.

The depth and plethora of information that data brokers collect and maintain on nearly everyone in the United States calls for strong privacy protections. The European Court of Human Rights (ECtHR) adopted an analysis of human rights that protects privacy interests in data while allowing government agencies to access people's private information in certain circumstances.[11] In this analysis, courts weigh the following factors: whether the surveillance is in accordance with the law; whether it "pursues . . . legitimate aims" stated in the law; and whether it is "necessary . . . in order to achieve" those aims.[12] This analysis also takes into account how the data is stored and accessed.[13]

The United States search warrant requirement does not go far enough, though there are signs that the Supreme Court is sympathetic to the ECtHR approach.[14] U.S. courts should adopt the ECtHR analysis when law enforcement agencies want to purchase people's data from data brokers. This analysis would likely first have to be adopted through congressional action due to its stark departure from the prevailing jurisprudence surrounding privacy rights in the United States.[15]

Part I of this Article will introduce some of the players in the data broker industry and describe the data that they collect. Part II will examine how law enforcement agencies use this information. Part III-A will discuss the current United States and ECtHR frameworks regarding how law enforcement agencies can use people's personal data, as well as other proposed solutions to this issue. Part III-B

[9] Morrison, *supra* note 5.

[10] *See* Lee Fang, *FBI Expands Ability to Collect Cellphone Location Data, Monitor Social Media, Recent Contracts Show*, THE INTERCEPT (June 24, 2020, 2:56 PM), https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/ [https://perma.cc/QHE4-EFH2].

[11] Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R., ¶ 332 (May 25, 2021).

[12] *Id.*

[13] *Id.* ¶ 335.

[14] Riley v. California, 573 U.S. 373, 402–03 (2014).

[15] *See id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

will demonstrate why the ECtHR framework should be applied in the United States, particularly considering the kinds of information that data brokers sell to law enforcement agencies. Part III-C will examine and critique reasons as to why law enforcement agencies should possibly be allowed to continue this practice under current Fourth Amendment jurisprudence. Finally, Part IV will explore how the ECtHR framework might work in practice in the United States, as applied to the examples provided in Part II of this Article.

I. BACKGROUND

There are many data brokers in the United States.[16] Some of them are relatively unknown outside of the industry and do nothing except obtain and sell data, while others are well-known companies that sell people's data in addition to offering their primary products.[17] Data brokers collect a wide range of information, some of which is relatively easy to obtain, and some of which could be damaging if made public.[18]

A. The Companies that Know Everything About You

Located in the middle of Arkansas is Acxiom, which describes itself as a "customer intelligence company" that collects data for marketers.[19] In 2012, analysts said that Acxiom's collection of consumer data was the largest in the world, representing approximately 500 million people,[20] including the data of most adults in the United States.[21] Acxiom made over $77 million that year selling data to numerous clients, including well-known companies such as Wells Fargo, Toyota, and Macy's.[22]

[16] *See* Zachary McAuliffe, *Data Brokers and Personal Data Deletion Services: What You Should Know*, CNET (Feb. 22, 2023, 5:00 AM), https://www.cnet.com/tech/services-and-software/data-brokers-and-personal-data-deletion-services-what-you-should-know/ [https://perma.cc/2M5D-6FKM]; *see also These Are the Largest Data Brokers in America*, PRIVACYBEE, https://privacybee.com/blog/these-are-the-largest-data-brokers-in-america/ [https://perma.cc/7MV2-AFWG] (last visited May 8, 2023).

[17] *See* McAuliffe, *supra* note 16.

[18] *Id.*

[19] Acxiom, LINKEDIN, https://www.linkedin.com/company/acxiom/about [https://perma.cc/9EVL-Z82X] (last visited May 8, 2023).

[20] Singer, *supra* note 4.

[21] *Id.*

[22] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

Some data brokers target particular types of data instead of focusing on everything. ZoomInfo collects information about various companies and their employees,[23] with the goal of selling this information to marketing companies.[24] However, similar to Acxiom, ZoomInfo is not small: it stores data consisting of various metrics, including contact information for influential employees, on approximately fourteen million companies.[25] It then sells this data to over 15,000 companies to help them "sell and market more efficiently and effectively."[26]

Certain companies are known for offering a particular product or service, but they also sell people's information. For example, Experian is one of the three major credit reporting agencies in the United States.[27] In this role, Experian keeps track of information relating to people's creditworthiness, as based on an individual's tax liens, history of bankruptcy, and repayment history.[28] However, Experian and the two other major credit reporting agencies also sell information to other companies that want to market their own products.[29] Further, Experian has an entire corporate division dedicated to selling consumer data.[30] This information goes far beyond the data that it uses to determine someone's credit score.[31]

On the other side, certain companies use information from data brokers to create targeted ads. Facebook is free for the everyday user, but it earns money from

[23] *See Contact Company Search*, ZOOMINFO, https://www.zoominfo.com/solutions/contact-company-search [https://perma.cc/3HUD-7EMD] (last visited May 8, 2023).

[24] *See About Us*, ZOOMINFO, https://www.zoominfo.com/about [https://perma.cc/7Z75-C5A6] (last visited May 8, 2023).

[25] *ZoomInfo Announces Secondary Offering of Shares of Class A Common Stock*, BUS. WIRE (Nov. 30, 2020, 7:33 AM), https://www.businesswire.com/news/home/20201130005535/en/ZoomInfo-Announces-Secondary-Offering-of-Shares-of-Class-A-Common-Stock [https://perma.cc/3UF5-F9UT].

[26] *Id.*

[27] Latoya Irby, *What Are the 3 Major Credit Reporting Agencies?*, THE BALANCE (Feb. 25, 2020), https://www.thebalance.com/who-are-the-three-major-credit-bureaus-960416 [https://perma.cc/4DWJ-A4BB].

[28] *Id.*

[29] *Id.* Equifax, however, distinguishes between information that it sells subject to the Fair Credit Reporting Act and information that it sells for other purposes. *See Equifax Privacy Statement*, EQUIFAX, https://www.equifax.com/privacy/privacy-statement/ [https://perma.cc/DS4R-75KA] (last visited May 8, 2023).

[30] *See Supercharge Your Marketing Campaigns with the Power of Data*, EXPERIAN, https://www.experian.com/marketing-services/index [https://perma.cc/MX8D-6P9B] (last visited May 8, 2023).

[31] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

advertisers when people use the platform and view advertisements embedded within the platform.[32] Facebook claims that it does not sell people's data,[33] but it does obtain information about its users from third parties.[34] Facebook combines the information that users themselves add to the platform with information from third parties, which in turn allows marketers to create advertisements that are targeted to a particular audience.[35]

B. Nothing Is Hidden

Companies that collect and sell people's personal data have access to a multitude of sources. Some of the data comes from public records,[36] some comes from information that users themselves reveal to the company (either on purpose or inadvertently),[37] and additional data comes from yet other companies that sell information.[38]

The specific data that these data brokers collect runs the gamut. It includes email addresses and political party affiliation, along with loyalty brand credit card purchases and income information.[39] Some data brokers also compile information about someone's children, if any, as well as religious beliefs, any pets someone may own, and clothing sizes.[40] Some companies even sell information about people who

[32] *See Market Your Business on Facebook and Increase Sales*, FACEBOOK, https://www.facebook.com/business/marketing/facebook [https://perma.cc/DZ4T-7HCC] (last visited May 8, 2023).

[33] Ina Fried, *What Facebook Knows About You*, AXIOS (Jan. 2, 2019), https://www.axios.com/facebook-personal-data-scope-suer-privacy-de15c860-9153-45b6-95e8-ddac8cd47c34.html [https://perma.cc/V7JX-J9XH].

[34] *Id.*

[35] *Id.*

[36] Steven Melendez & Alex Pasternack, *Here are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/R8BE-HCFC].

[37] *Id.*

[38] *Id.*

[39] WebFX Team, *What are Data Brokers—And What is Your Data Worth? [Infographic]*, WEBFX (Mar. 16, 2020), https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ [https://perma.cc/H2H9-KN2N].

[40] Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records*, WIRED (June 27, 2018, 1:34 PM), https://www.wired.com/story/exactis-database-leak-340-million-records/ [https://perma.cc/PMC8-FKXW].

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

suffer from sensitive health conditions, such as erectile dysfunction or HIV/AIDS,[41] and can potentially infer someone's sexual orientation based on where that person purchases particular products and which bars they frequent.[42]

Once data brokers obtain this information, it is difficult for people to remove it from the companies' databases. The Fair Credit Reporting Act requires that some companies honor requests to delete data, but otherwise, individual data brokers can require people to complete several steps in order to have their data removed.[43] There are also separate companies that charge a fee to remove someone's information for them, and sometimes, at an extra cost, keep that information out of those databases after that initial removal.[44]

Some data brokers provide descriptions of where they obtain their data, as well as the general categories of data they collect. For example, Acxiom obtains data from public sources, such as websites and real property records, and says that the company also collects information from other data brokers.[45] The company collects personal identifying information, such as shopping activity and geolocation data, and creates profiles about consumers based on this data.[46] Acxiom also says that it sells this information to companies across a variety of industries, including financial institutions, universities, and government agencies.[47] Some of this data can reveal information that people would rather keep private. Geolocation data in particular can identify details that one would rather keep to oneself, such as visits to Planned

[41] Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers,'* FORBES (Dec. 19, 2013, 3:40 PM), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/ [https://perma.cc/3S7K-AAAN].

[42] Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS (Mar. 9, 2014, 7:09 PM), https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ [https://perma.cc/9CZP-8DFT].

[43] *See* Melendez & Pasternack, *supra* note 36.

[44] David Nield, *How to Opt out of the Sites That Sell Your Personal Data*, WIRED (Nov. 7, 2019, 11:00 AM), https://www.wired.com/story/opt-out-data-broker-sites-privacy/ [https://perma.cc/4AAF-KTAF].

[45] *US Products Privacy Notice*, ACXIOM, https://www.acxiom.com/about-us/privacy/highlights-for-us-products-privacy-policy/ [https://perma.cc/8TRK-4NDH] (last visited May 8, 2023).

[46] *Id.*

[47] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

Parenthood or a Weight Watchers meeting.[48] Although that data might be anonymized, it is often still possible to connect it with a specific person by analyzing patterns of behavior or other information.[49]

Some data brokers are more transparent about the kinds of data that they collect and then sell. One data broker called Statlistics maintains lists of various kinds of data that are available for purchase, sorted alphabetically.[50] Companies can purchase lists of people who subscribe to acoustic guitar magazines,[51] postal addresses and email addresses for C-suite casino managers,[52] and names, genders, and addresses of undergraduate students who are members of the Association for Psychological Science,[53] among many other sets of data.

II. FEDERAL USE OF THIRD-PARTY DATA

In *Carpenter v. United States*, the Supreme Court held that government officials must obtain a search warrant if they want to request from carriers seven or more days of geolocation data generated by someone's cell phone.[54] To circumvent the need for a warrant, federal law enforcement agencies make use of information provided by data brokers, particularly geolocation data.

Many federal agencies take advantage of this loophole and extensively rely on data from data brokers. For example, the Department of Homeland Security (DHS) purchased geolocation data obtained by Venntel, a data broker that partners with Gravy Analytics, a large advertising company.[55] DHS then used the data to perform

---

[48] *See, e.g.*, Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/H49T-FSE5].

[49] *See id.*

[50] *See Data Card Search*, STATLISTICS, https://www.statlistics.com/data-card-search.html [perma.cc/2MSN-T599] (last visited May 8, 2023).

[51] *Acoustic Guitar Magazine*, STATLISTICS, https://www.statlistics.com/mailing-lists/acoustic-guitar.html [perma.cc/XU3N-5CW7] (last visited May 8, 2023).

[52] *Gambling & Casino Industry Trends*, STATLISTICS, https://www.statlistics.com/mailing-lists/gambling-and-casino-industry-trends.html [perma.cc/B2S5-WLRZ] (last visited May 8, 2023).

[53] *Undergraduate Psychology Students from APS*, STATLISTICS, https://www.statlistics.com/mailing-lists/undergraduate-psychology-students-from-aps.html [perma.cc/A2X4-LTRJ] (last visited May 8, 2023).

[54] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[55] Tau & Hackman, *supra* note 8.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

immigration enforcement actions, which led to the arrests of several people who had entered the United States without authorization.[56] DHS has also used the data to prevent human- and drug-trafficking operations.[57] For example, people who were familiar with the usage of this data said that it was used in 2018 to arrest a drug trafficker in Arizona, although local police records did not indicate that they relied on that data.[58]

This loophole is not limited to DHS and its constituent agencies. The Secret Service has used the same technique, perhaps in an attempt to avoid the search warrant requirement.[59] The agency utilized geolocation data provided by Babel Street, which collects that data from different apps on people's phones.[60] According to Babel Street, in 2018, the Secret Service used the data to find and disable nearly 200 credit card skimmers before Thanksgiving.[61]

Law enforcement agencies' use of geolocation data provided by data brokers is not limited to preventing drug trafficking or enforcing immigration laws, as DHS has done,[62] or to tracking people who are suspected of other crimes. The Federal Bureau of Investigation (FBI) has used and continues to use data provided by Venntel to surveil people who are not necessarily under investigation for committing any particular crime.[63] This data can be highly accurate, potentially allowing law enforcement agencies to track somebody's location to within sixteen square feet,

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] Kate Cox, *Secret Service Buys Location Data That Would Otherwise Need a Warrant*, ARSTECHNICA (Aug. 17, 2020, 3:39 PM), https://arstechnica.com/tech-policy/2020/08/secret-service-other-agencies-buy-access-to-mobile-phone-location-data/ [https://perma.cc/MYC6-TU2].

[60] *Id.*

[61] *See* Charles Levinson, *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, PROTOCOL (Mar. 5, 2020), https://www.protocol.com/government-buying-location-data [https://www.protocol.com/government-buying-location-data]; *see also* Didi Martinez et al., *Secret Service Cracks Down on Credit Card Skimming at Gas Pumps Nationwide*, NBC NEWS (Nov. 23, 2018, 12:45 PM), https://www.nbcnews.com/news/us-news/secret-service-cracks-down-credit-card-skimming-gas-pumps-nationwide-n939496 [perma.cc/J5LX-7GJY].

[62] Tau & Hackman, *supra* note 8.

[63] *See* Fang, *supra* note 10.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

compared to traditional tracking data obtained from a cell phone carrier with a search warrant, which allows for tracking to within three-quarters of a square mile.[64]

Strictly law enforcement oriented agencies are not the only ones to use information provided by data brokers. The Internal Revenue Service (IRS) has used cell phone location data, also provided by Venntel, to attempt to find Americans who were suspected of violating tax laws.[65] The IRS Criminal Investigations Unit was able to cross-reference data points from various phones to see if they appeared at the locations of multiple suspicious transactions, and then follow the movements of any such phones.[66] The IRS had a subscription to Venntel's database during 2017 and 2018, but later said that it canceled the subscription because it did not help the IRS "locate any targets of interest."[67]

Law enforcement agencies do not always obtain their investigative data from data brokers. Sometimes, they use data from sources that obtained the data indirectly, such as through hacking. SpyCloud is a company that monitors when companies are hacked in order to help those companies protect their data.[68] SpyCloud itself does not hack those companies. However, after a company is hacked by other parties, SpyCloud then retains access to that hacked data and sells it to law enforcement agencies.[69] SpyCloud is not a data broker in the sense that it gathers people's data directly, but when law enforcement agencies purchase this data, they are relying on the same loophole that other federal agencies use when purchasing data from data brokers. Indeed, the Department of Justice relied on data provided by SpyCloud in a 2018 case involving DDoS-for-hire services in Los Angeles.[70]

---

[64] Bryon Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL ST. J. (June 19, 2020, 1:46 PM), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815 [perma.cc/P4WB-78YQ].

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Recaptured Data from Breaches, Botnets & Underground Sources*, SPYCLOUD, https://spycloud.com/our-data/ [https://perma.cc/4SSF-T3D5] (last visited May 8, 2023).

[69] Joseph Cox, *Police Are Buying Access to Hacked Website Data*, VICE (July 8, 2020, 9:29 AM), https://www.vice.com/en/article/3azvey/police-buying-hacked-data-spycloud [https://perma.cc/A5WR-CMUL].

[70] *Criminal Charges Filed in Los Angeles and Alaska in Conjunction with Seizures of 15 Websites Offering DDoS-for-Hire Services*, U.S. DEP'T OF JUST. (Dec. 20, 2018), https://www.justice.gov/opa/pr/criminal-

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

III. DISCUSSION

A. Relevant Laws and Potential Solutions

In the United States, law enforcement agencies generally must obtain a search warrant if they wish to search someone's data.[71] They must have probable cause to believe that the evidence they seek is located in the place where they will look.[72] However, information that is revealed to the public is no longer subject to the search warrant requirement.[73] In 2018, the Supreme Court held that, in certain cases, geolocation data from cell phones is subject to the search warrant requirement because such data can be highly sensitive.[74] However, law enforcement agencies have been exploiting loopholes in this area, as described above, by purchasing data from third parties instead of obtaining search warrants for that data.[75]

The ECtHR takes a different approach to this issue. When evaluating a government surveillance program, the court looks at whether the program is lawful, as well as necessary and proportional to a legitimate government aim.[76] For example, the court regards national security as a legitimate government aim, but also believes that there need to be limits on how governments collect, store, and use data for this purpose.[77] The court is also concerned about who has access to the data.[78] The Supreme Court of the United States may have begun to embrace the view that some kinds of information are so sensitive and reveal so much about a person that law enforcement agencies require a search warrant before obtaining access to that information, even if it is arguably public.[79] Nevertheless, the ECtHR approach in this

charges-filed-los-angeles-and-alaska-conjunction-seizures-15-websites-offering-ddos [https://perma.cc/DES9-7XVY].

[71] *See* U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 357 (1967).

[72] *See* U.S. CONST. amend. IV.

[73] *See Katz*, 389 U.S. at 361.

[74] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[75] Tau & Hackman, *supra* note 8.

[76] Klass and Others v. Germany, App. No. 5029/71, ¶¶ 42–43 (Sept. 6, 1978).

[77] Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R., ¶ 332 (May 25, 2021).

[78] *Id.* at 323.

[79] *See* Riley v. California, 573 U.S. 373, 402–03 (2014).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

area would protect people's privacy while still allowing law enforcement agencies to access the information they need.

Daniel J. Solove and Chris Jay Hoofnagle have put forth what they term a Model Privacy Regime to fix this problem.[80] Under their framework, all data brokers would first have to register with the Federal Trade Commission (FTC) and describe the kinds of information that they collect, as well as the entities to which they sell or otherwise disclose this information.[81] In response to the difficulties that many consumers face when trying to delete their data, Solove and Hoofnagle propose that data brokers must obtain informed consent from consumers before using that data, except as authorized by statute or to investigate fraud.[82] Solove and Hoofnagle also argue that the FTC should maintain a system similar to the Do Not Call registry so that people can easily prevent data brokers from using their information.[83] Law enforcement agencies would have to show probable cause to access the data and would only be able to access "as much information as necessary to meet the needs articulated in the showing of probable cause."[84]

This approach, along with the remainder of the Model Privacy Regime framework,[85] could effectively protect people's personally identifying information from the regular machinations of data brokers by placing greater burdens on the collection and distribution of data. However, it contains exceptions for "reasonable law enforcement needs" without specifying what those needs are or what reasonable means in this context.[86] Additionally, their proposal regarding prospective crimes, such as the surveillance that the FBI conducted using Venntel data,[87] defers to the existing legal regime,[88] which fails in this area. As such, this approach would likely

[80] Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357 (2006).

[81] *Id.* at 368–69.

[82] *Id.* at 369.

[83] *Id.* at 370.

[84] *Id.* at 370–71.

[85] *See id.* at 371–403.

[86] *Id.* at 377–78.

[87] Fang, *supra* note 10.

[88] Solove & Hoofnagle, *supra* note 80, at 378.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

not prevent data brokers from selling people's information to law enforcement agencies.

On the other hand, Alexander Tsesis takes the position that the United States should adopt the European Union's "right to erasure."[89] He points out that it is difficult for consumers to have any control over where their online data goes after it gets onto the internet.[90] He also explores internet browsers' use of cookies and argues that because consumers do not know how to prevent websites from storing cookies on their computers, they have no say over whether websites will monitor, and later sell, details about their internet usage.[91] Further, Tsesis describes the various ways in which data brokers can track and store information about people's personal lives, such as their "shopping habits, relationships, browsing histories, [and] family backgrounds."[92] Tsesis then points out that there are no laws that require data brokers to delete any of this information.[93] The potential for abuse of this data,[94] according to Tsesis, justifies someone's right to have that data deleted in certain cases, such as when the person revealed that information voluntarily.[95] This would only apply to certain kinds of data, such as private information that was later shared or sold without that person's permission.[96]

This proposal does not apply specifically to law enforcement, but it could serve as a check on law enforcement agencies' use of some personal data. However, as Tsesis himself states, it would not apply to public data.[97] As such, any right to erasure under this framework would be limited. Depending on how courts, legislatures, and law enforcement agencies themselves interpret data as public or private,[98] law

[89] Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433 (2014).

[90] *See id.* at 437–38.

[91] *See id.* at 438–39.

[92] *See id.* at 440–41; *see also supra* Part I–B.

[93] *See* Tsesis, *supra* note 89, at 441. *But see California Consumer Privacy Act (CCPA)*, CAL. DEP'T OF JUST.—ATT'Y GEN. (Feb. 15, 2023), https://oag.ca.gov/privacy/ccpa [https://perma.cc/7RKB-GVU5].

[94] Tsesis, *supra* note 89, at 454.

[95] *See id.* at 479.

[96] *See id.* at 480.

[97] *Id.*

[98] *See infra* text accompanying notes 113–114.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

enforcement agencies could still have access to a large amount of data, and consequently, this proposal would have no real effect. Furthermore, this deletion would apply to the companies holding the data, but not necessarily to law enforcement agencies after data brokers have already sold the data.[99] Therefore, it is more feasible to have a general framework that governs the usage of all data in the first place without trying to specify which kinds of data should be protected and which kinds are acceptable to use.

Senators Ron Wyden and Rand Paul, along with eighteen other senators, co-sponsored the Fourth Amendment is Not for Sale Act, which would ostensibly close the loophole discussed in this Article by requiring law enforcement agencies to obtain a search warrant before purchasing data from data brokers.[100] However, this bill still does not fully protect Americans' data privacy. The bill would require intelligence agencies to go through the process detailed in the Foreign Intelligence Surveillance Act (FISA) in order to obtain data on location and internet history "for foreign intelligence purposes."[101] Activists and journalists have documented numerous problems with the FISA process,[102] and the ECtHR framework provides stronger protections in this area.[103] The bill also does not address how law enforcement agencies should store such data or who has access to it, which could lead to other problems discussed in this Article.[104]

[99] *See infra* text accompanying note 107.

[100] Press Release, Ron Wyden, Senator, United States Senate, Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not for Sale Act (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act- [https://perma.cc/58VX-4AYG].

[101] S. 1265, 117th Cong. § 5 (2021).

[102] *See, e.g.*, Ryan Lucas, *Justice Department IG Finds Widespread Problems with FBI's FISA Applications*, NPR (Mar. 31, 2020, 1:37 PM), https://www.npr.org/2020/03/31/824510255/justice-department-ig-finds-widespread-problems-with-fbis-fisa-applications [https://perma.cc/3MNZ-VFCW]; David Ruiz, *The Problems with FISA, Secrecy, and Automatically Classified Information*, ELEC. FRONTIER FOUND. (Feb. 26, 2018), https://www.eff.org/deeplinks/2018/02/problems-fisa-secrecy-and-automatically-classified-information [https://perma.cc/87BB-ZRT6].

[103] Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R. (May 25, 2021).

[104] *See infra* text accompanying note 117.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

B. Information Obtained from Data Brokers Is so Invasive that It Should Be Governed Under the ECtHR Framework

Law enforcement agencies' use of data obtained from data brokers presents two issues: (1) the initial access of data, and (2) the subsequent use of data. One can argue that it is problematic for law enforcement agencies to even have access to these databases in the first place, while others may argue that unless the information is used inappropriately, there is nothing wrong with it. Regardless, law enforcement agencies try to use this data for law enforcement purposes, so there should be a governing framework in accordance with the Fourth Amendment to ensure that law enforcement agencies can only access and use the data in appropriate circumstances.

Law enforcement agencies' purchase and usage of this information arguably constitutes a surveillance program.[105] As stated above, data brokers have information about millions of people in the United States and around the world.[106] Because information from data brokers can reveal private details about a person—including their historical locations, their hobbies, and their medical history—the ECtHR analysis should be applied to determine whether law enforcement agencies should be allowed to purchase and use information from data brokers. Under the ECtHR framework, to prevent law enforcement officials from potentially abusing this data, courts would need to determine whether access to all of this information is necessary in order to achieve their goals.[107] As demonstrated by the failure of the IRS's Criminal Investigations Unit to arrest, charge, and convict a single person of a tax-related crime based on access to location history,[108] it is not always necessary for law enforcement agencies to have access to the amount of information that they currently do.

Similarly, it is difficult for people to delete their information from the data brokers' databases.[109] Once law enforcement agencies obtain it, it is conceivable that the data will never be deleted; even if one can remove information from the data brokers' possession, the law enforcement agency's copy of the data does not necessarily reflect that removal. Current Fourth Amendment case law does not

[105] *See, e.g.*, Fang, *supra* note 10.

[106] *See* Singer, *supra* note 4.

[107] Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R. (May 25, 2021).

[108] *See* Tau, *supra* note 64.

[109] *See* Melendez & Pasternack, *supra* note 36.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

address this issue. As such, the ECtHR approach would serve as a better framework in this area.

Additionally, the fact that at least some of the data is anonymized does not negate the fact that it can reveal sensitive information about someone.[110] That revelation is arguably not necessary for a legitimate government aim. For example, when law enforcement agencies purchase location data, they are not obtaining information about only one person.[111] Rather, they obtain access to databases containing data about millions of people, despite being facially interested in only a small fraction of that data.[112] Under the ECtHR approach, law enforcement agencies would only be allowed to access the information of people who are specifically suspected of a crime, except in certain cases where it is necessary to collect more data, to the extent justified by probable cause.[113] This would protect the millions of other people who either do not know about the pervasive collection of data by the government or cannot stop data brokers from sharing their information.

C. But if the Fourth Amendment Does Not Apply, Why Cannot Law Enforcement Agencies Purchase this Data?

One argument in favor of law enforcement agencies being allowed to purchase and use this data is that the data is public, or at least not held solely by the party who is the subject of the data.[114] This is true for public records, and possibly for many individual data points in these databases—for example, one can argue that if a company lists its employees on its website, that information is public, and law enforcement agencies are not doing anything wrong by buying this information from companies like ZoomInfo.[115] However, when multiple data points are combined, they provide a very detailed depiction of someone's personal life, much more so than

[110] *See* Valentino-DeVries et al., *supra* note 48.

[111] *See* Tau & Hackman, *supra* note 8.

[112] *See id.*

[113] *See infra* text accompanying note 118.

[114] *See* Sharon Bradford Franklin & Dhanaraj Thakur, *New CDT Report Documents How Law Enforcement Agencies Are Evading the Law and Buying Your Data from Brokers*, CTR. DEMOCRACY & TECH. (Dec. 9, 2021), https://cdt.org/insights/new-cdt-report-documents-how-law-enforcement-intel-agencies-are-evading-the-law-and-buying-your-data-from-brokers/ [https://perma.cc/PWQ5-EBN7].

[115] ZOOMINFO, https://www.zoominfo.com/data-sources [https://perma.cc/TUN6-9DJ9] (last visited May 8, 2023).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

would be possible from any single data point.[116] As such, it might be better to look at this data as more than individual, unique data points. Rather, when all of this data is combined, law enforcement agencies have access to information that is arguably private in the aggregate, especially because some data brokers create inferences based on the data that they have[117]—and data about these inferences is not entirely public. Therefore, although some of the information in any given individual profile might be publicly available, the combination of that data effectively creates private information. The Fourth Amendment might not stop government entities from buying information from third parties, but the ECtHR analysis is well-suited to dealing with this issue.

According to DHS and other law enforcement agencies, the government is acting like a private citizen in these cases, since they are purchasing data that is commercially available, and therefore, there should be no problem for the government agencies to do so.[118] However, this argument misses the point. The key issue is not whether the government is acting like a private entity. Rather, the issue, for Fourth Amendment purposes, is whether this data is essentially private. The combination of all of this data can be more revealing than any single data point, and there are strong reasons to be concerned about how the government can misuse that information, especially when that information is utilized for law enforcement purposes.[119] Additionally, although the Fourth Amendment only applies to searches conducted by or on behalf of the government,[120] there should be guidelines in place whenever the government obtains access to people's personal information and uses that information to further objectives related to law enforcement. There is a gap between traditional searches conducted under the Fourth Amendment and situations where the government has access to the same information from other sources, such

[116] *See, e.g.*, EXPERIAN, https://www.experian.com/marketing-services/targeting/data-driven-marketing/consumer-view-data [https://perma.cc/VXS4-LK3S] (last visited May 8, 2023); Valentino-DeVries et al., *supra* note 48.

[117] *See US Products Privacy Notice*, *supra* note 45.

[118] *See* Tau & Hackman, *supra* note 8.

[119] *See, e.g.*, *Across U.S., Police Officers Abuse Confidential Databases*, AP NEWS (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43 [https://perma.cc/SYM4-D9FT].

[120] Barry Friedman & Orin Kerr, *The Fourth Amendment: Common Interpretation*, NAT'L CONST. CTR., https://constitutioncenter.org/the-constitution/amendments/amendment-iv/interpretations/121 [https://perma.cc/WKB5-ZPL] (last visited May 8, 2023).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

as when the government can purchase the same data as anyone else, and the ECtHR analysis would fill that gap.

However, buying information from data brokers can allow law enforcement agencies to obtain this information more quickly, more cheaply, and more efficiently than if they had taken the time to get a search warrant—especially if they already have all of the data on hand for future needs.[121] Speed is important in urgent cases, such as a kidnapping or an imminent terrorist attack, and having information on hand can make a difference in the outcome. Nevertheless, this defeats the purpose of the search warrant requirement in the first place. The purpose of requiring a search warrant is that the government has to demonstrate that it has probable cause to look at this information, not just because something might happen at some point in the future.[122] The ECtHR analysis would neatly solve this problem: if the government can show that it needs specific information on hand for the purpose of a legitimate government aim, such as solving kidnappings and preventing terrorism, then it can purchase the information and store it. Otherwise, law enforcement agencies should not be allowed to purchase and store this information from data brokers.

IV. FOURTH AMENDMENT IMPLICATIONS AND LEGITIMATE GOVERNMENT AIMS

The ECtHR analysis, if applied to situations where U.S. law enforcement agencies need access to this data, would still not replace the Fourth Amendment. In cases involving requests for data directly from the source, such as cell phone carrier records or a suspect's phone's location log, the Fourth Amendment would still apply.[123] However, in cases involving requests for data from third parties that already have that data on hand, such as data brokers, the ECtHR analysis would apply. Additionally, the ECtHR analysis would apply to any storage of such data, since the Fourth Amendment only deals with requests for search warrants in the first instance.[124] Thus, the ECtHR analysis would bridge the gap between cases where the Fourth Amendment applies and cases where it does not.

In practice, it would sometimes be possible for a U.S. law enforcement agency to conform with the ECtHR analysis and sometimes not. For example, in cases where

[121] *See Accelerate Your Investigations*, CLEARVIEW AI, https://www.clearview.ai/law-enforcement [https://perma.cc/YQ8E-7XK4] (last visited May 8, 2023).

[122] Friedman & Kerr, *supra* note 120.

[123] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[124] Friedman & Kerr, *supra* note 120.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

DHS uses cell phone location data for immigration enforcement purposes,[125] DHS would first have to demonstrate that it is necessary to use data provided by third parties instead of obtaining a search warrant (assuming that there is a federal law that sanctions this program in the first place). Under Big Brother Watch,[126] DHS could argue that immigration enforcement is important to national security, which is a legitimate government aim, and further, that it is therefore necessary to have a collection of data on hand, instead of taking the time to obtain a search warrant.

A similar analysis would apply in the case of the Secret Service using Babel Street's location data.[127] The Secret Service would have to show that it must use third-party data instead of going to the cell phone carriers with a search warrant. Stopping credit card skimmers is arguably a legitimate government aim, especially because skimmers usually target gas stations, which, according to the Secret Service, could have affected approximately fifty-four million Americans when the Secret Service used this data.[128] In this case, it might not have been feasible to obtain a search warrant because the Secret Service might not have known exactly who was installing the credit card skimmers, only that people were doing so in the first place and that the agency needed to find out who was in the area surrounding the affected gas stations.

The IRS Criminal Investigations Unit might be allowed to use cell phone location data provided by data brokers under the ECtHR analysis.[129] Preventing tax fraud is arguably a legitimate government aim. Additionally, just like the Secret Service's use of such data, the IRS might not have known exactly who was making the suspicious transactions, only that they were occurring. However, the IRS admitted that they did not see any results from that data.[130] As such, use of this data might in fact not be a necessary method of achieving the legitimate government aim of preventing tax fraud, at least in similar future cases without any specific suspects.

---

[125] Tau & Hackman, *supra* note 8.

[126] Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R., ¶ 347 (May 25, 2021).

[127] Cox, *supra* note 59.

[128] *See* Martinez et al., *supra* note 61.

[129] *See* Tau, *supra* note 64.

[130] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

However, the ECtHR analysis would likely prevent the FBI from surveilling people who are not suspected of a particular crime.[131] National security is a broad umbrella category under Big Brother Watch, but there are other tools available besides storing databases of people's location history and other personally identifiable information. As such, it is not necessary and proportionate for the FBI to use Venntel's data to surveil people who have no connection to a particular crime.

CONCLUSION

Allowing law enforcement agencies to purchase databases containing the data of millions of Americans, without requiring them to first obtain a search warrant, is an end run around the Fourth Amendment and should be subject to strict guidelines. The ECtHR approach would solve this problem. However, implementing this in practice may be difficult. For one, the Supreme Court has not said definitively that law enforcement having access to large amounts of personal data is a problem (the sentiment in *Riley* remains dicta, for now).[132] As such, American courts and legislators might not perceive a need to fix anything about the current legal regime. Additionally, "legitimate government aim" is a large category, one that even European courts have expanded, and includes national security,[133] which can encompass many different areas, needs, and uses. This can effectively render the ECtHR framework toothless in the United States. Nevertheless, some members of Congress have begun to investigate this issue, particularly the IRS's use of location data.[134]

The FTC has already recommended that Congress regulate the data broker industry.[135] Some of those suggestions mimic Solove and Hoofnagle's Model Privacy Regime.[136] In particular, the FTC suggested that Congress pass legislation to create a central location that lists data brokers, require that data brokers allow

[131] *See* Fang, *supra* note 10; *see also* Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, and 24960/15, Eur. Ct. H.R., ¶ 347 (May 25, 2021).

[132] *See* Riley v. California, 573 U.S. 373 (2014); *see also* United States v. Shipton, 5 F.4th 933, 936 (8th Cir. 2021).

[133] Klass and Others v. Germany, App. No. 5029/71, ¶¶ 42–43 (Sept. 6, 1978).

[134] Tau, *supra* note 64.

[135] Press Release, Federal Trade Commission, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control over Their Personal Information (May 27, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more [https://perma.cc/ZWR3-YJK3].

[136] Solove & Hoofnagle, *supra* note 80, at 368–82.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu

consumers to view their data and suppress its usage, and "obtain affirmative express consent from consumers before" collecting various kinds of sensitive information, such as health-related information.[137] However, the same problems with the Model Privacy Regime apply to these proposals.[138]

The problem may lie in the fact that the U.S.'s privacy model is different than Europe's.[139] For example, as Professor Tsesis points out, European countries were concerned about protecting unauthorized disclosure of someone's data even before the internet was created.[140] As such, attempts to work within the framework of U.S. privacy laws and principles will inevitably lead to loopholes that can be exploited both by data brokers and law enforcement agencies. The ECtHR approach represents a change from the way that the United States typically approaches data privacy, but it may be the best way to protect people's personal data from being used against them by law enforcement agencies.

[137] Press Release, FTC, *supra* note 135.

[138] *See supra* text accompanying notes 85–87.

[139] *See* Tsesis, *supra* note 89, at 463.

[140] *See id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2023.968
http://lawreview.law.pitt.edu