Duke SANFORD | CYBER POLICY PROGRAM

Data Brokers and Sensitive Data on U.S. Individuals

Threats to American Civil Rights, National Security, and Democracy

By Justin Sherman

—

Overview: This report examines 10 major data brokers and the highly sensitive data they hold on U.S. individuals. It finds that data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees. It first describes the problem of virtually unregulated data brokerage in the United States. It then describes the findings of research conducted for this paper on data brokers openly and explicitly advertising sensitive data on U.S. individuals, including a specific analysis of data relating to military personnel. It then concludes with policy implications for the United States—including ways this data collection, aggregation, selling, and sharing threatens civil rights, national security, and democracy.

Author: Justin Sherman is a cyber policy fellow at Duke University's Technology Policy Lab, where he directs the data brokerage research for Duke's Privacy & Democracy Project.

Publication Note: The author's views are their own and also reflect the broader position of the Duke University Sanford Cyber Policy Program. These views do not necessarily represent those of the Duke University Sanford School of Public Policy or Duke University. This paper was produced intellectually independently as part of the data brokerage research team for Duke's Privacy & Democracy Project.[1]

Overview of Problem and U.S. Congress Response

Problem: Data brokerage—broadly, the practice of buying, aggregating, selling, licensing, and otherwise sharing individuals' data—is a virtually unregulated practice in the United States. Major data brokerage firms are presently offering reams of data on U.S. individuals for sale, and virtually nothing in current U.S. law limits their selling that data to a range of actors, from insurance firms to U.S. law enforcement agencies to foreign entities. This data could be used for a range of activities that violate Americans' civil rights, hurt U.S. national security, and threaten democracy itself.

> **Data Brokers:** There is no single, agreed-upon definition of data brokers in United States law. Vermont and California have their own definitions in state laws that require "data brokers" to register with the state; these laws create a distinction between firms engaged in the general practice of data brokerage (buying, selling, licensing, etc. data) and those that specifically qualify as "data brokers," which effectively exempts many companies that buy and sell data from complying with the state's data broker disclosure requirements, because they do not have the narrow "data broker" characteristics. The Federal Trade Commission (FTC) offers its own non-statutory definitions in policy reports, which do not make this same distinction.[2]
>
> **Data Gathering Mechanisms:** Data brokers may gather data on individuals directly, from firms they own and/or software applications they control. Data brokers may also purchase, license, or otherwise acquire data second-hand from companies that directly collect this information from their users. They may also crawl government records to develop profiles on individuals (most often seen on "white pages" or "people-search" websites). U.S.-incorporated data brokers often advertise data on U.S. individuals as well as on individuals from many other countries globally.
>
> **Data Sharing Mechanisms:** Data brokers typically offer pre-packaged databases of information to potential buyers. These databases are packaged along a variety of lines, ranging from the personal preferences and behaviors of the individuals to their specific occupations and roles in society (e.g., military personnel). In addition to outright selling data on individuals, data brokers may also license and otherwise share the data with third parties. There is, at present, limited visibility into data brokerage transaction processes beyond information reported by journalists.

Policy Response: The U.S. Congress should consider giving the executive branch export control authorities to limit potential data broker sales of sensitive data on U.S. individuals to foreign governments and to non-state actors with close ties to foreign intelligence and security agencies. The U.S. Congress should also make data brokerage a central part of robust federal privacy legislation that establishes rules around and implements restrictions on the private collection, aggregation, sale, licensing, and sharing of U.S. individuals' data—including placing limits on federal government purchasing of data broker data and giving the Federal Trade Commission further authority to investigate unfair and exploitative data broker practices and use of data broker data by other firms.

Research Findings

Overview:

- All 10 surveyed data brokers openly and explicitly advertise data on millions of U.S. individuals, oftentimes advertising thousands or tens of thousands of sub-attributes on each of those individuals, ranging from demographic information to personal activities and life preferences (e.g., politics, travel, banking, healthcare, consumer goods and services)
- People-search websites aggregate public records on individuals and make it possible for anyone to search for major activist figures, senior military personnel, and other individuals—uncovering home address, phone number, and other information as well as the names of known family members and relatives
- Oracle has a data partner that openly and explicitly advertises data on U.S. individuals' interest in political organizations, figures, and causes, including but not limited to data on those who support the National Association for the Advancement of Colored People (NAACP), Planned Parenthood, the American Civil Liberties Union (ACLU), and the National LGBTQ Task Force
- Oracle, Epsilon, and other data brokers openly and explicitly advertise data sharing platforms to which anywhere from dozens to thousands of companies contribute data on individuals
- Multiple data brokers advertise the ability to locate individuals, ranging from the use of driver license records and other aggregated data to pinpointing phone geolocations
- Three major U.S. data brokers, Acxiom, LexisNexis, and Nielsen, openly and explicitly advertise data on current or former U.S. military personnel; LexisNexis advertises a capability to search an individual and identify whether they are active-duty military; and other brokers likely sweep up military personnel in their larger data sets

Data Broker	Headquartered
Acxiom	U.S.
LexisNexis	U.S.
Nielsen	U.S.
Experian	Ireland
Equifax	U.S.
CoreLogic	U.S.
Verisk	U.S.
Oracle	U.S.
Epsilon	U.S.
People-search sites	Many in U.S.

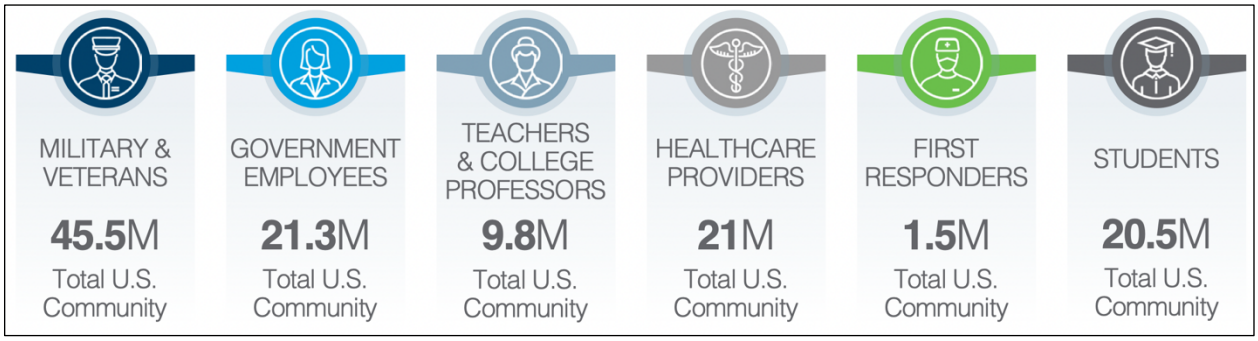
Research Methodology: The author created a list of 10 large data brokers, based on information compiled by research assistants. The author then searched through the publicly available documentation on these data brokers, including promotions and marketing materials on their own public websites, to document their advertising of data on U.S. individuals. The author also wrote a short analysis of people-search websites, based on a survey of multiple major people-search (aka "white pages") websites. There are many

smaller and potentially less reputable data brokers, but this research focused on the largest, well-known data brokers as well as people-search websites due to their visibility.

—

Acxiom: Broadly, Acxiom advertises data coverage of over 62 countries and the ability to reach over 2.5 billion consumers globally.[3] It advertises data attributes on individual demographics (age, gender, ethnicity, education, occupation), household characteristics (household size, number/ages of children), financial data (income ranges, net worth, economic stability), life events (marriage/divorce, birth of children, moves), interests (sports, leisure activities, family, pets, entertainment), buying activities (products bought, method of payment), behavior (community involvement, causes, gaming), major purchases (automotive, home purchase), and geospatial insights (geocoding of latitude/longitude, Census data aggregated at Block, Tract, DMA, ZIP+4).[4] This data also includes over 225 million landline and wireless telephone numbers in the U.S. and Canada and over 965 million U.S.-based consumer records, including the ability to link emails and names to postal addresses.[5]

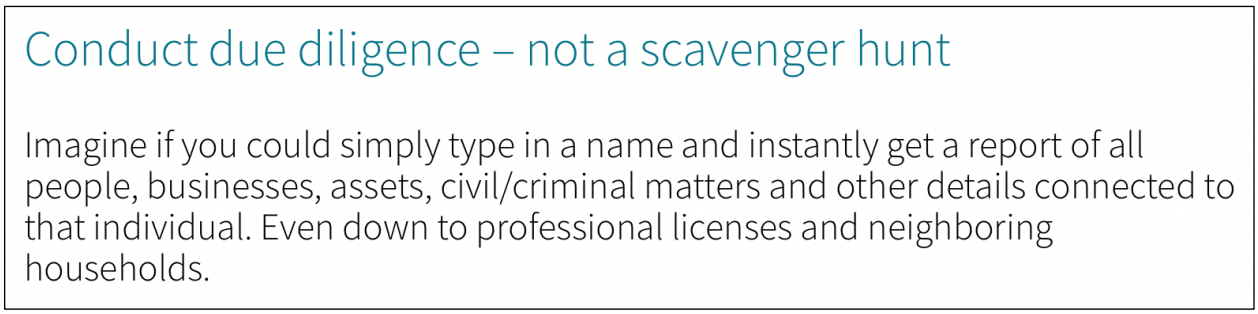
Acxiom explicitly advertises data on 45.5 million current and former U.S. military personnel. It advertises a marketing service for clients to send "gated offers" to those individuals, by identifying the intended audience, defining the offer, specifying the channels used for outreach, and establishing the timing of the offer; after this point, Acxiom says it will map out an implementation plan that can go live in as few as 45 days.[6] Acxiom also offers "verification and location of military servicemen (deployed but missing from base)" as part of commercial work for credit card issuers and retail banks.[7]



Advertisement of Acxiom's data on active and former U.S. military personnel. July 2021.

LexisNexis: LexisNexis advertises data on 270 million transactions around the globe each hour and data linked to over 283 million active U.S. consumer profiles.[8] It advertises data from 1.5 billion bankruptcy records, 77 million business contact records, 330 million unique cell phone numbers, 11.3 billion unique name and address combinations, 6.6 billion motor vehicle registrations, and 6.5 billion personal property records.[9] It advertises the ability to "identify relatives, associates and neighbors who may show up in photos or be mentioned in social media postings with a search of hundreds of networks and millions of sites on the open web."[10] It also advertises the ability to "determine a person's current whereabouts" using recent driver license records.[11]

LexisNexis advertises data related to "crime and criminal investigations," including the ability to "instantly search detailed information using data from over 37 billion public records and 10,000 disparate sources" and the ability to process thousands of records at a time. It advertises the ability to filter and link "billions of records to provide a more complete picture of an individual," including to "find connections between people and their assets, relatives and business associates."[12] It advertises customizable alerts of changes to data in an individuals' profile, "state and regional-specific" data sets in addition to public records on individuals, and the ability to, "in minutes, confidently identify, confirm and authenticate identities" for individuals ("especially useful for individuals with common names").[13] It says its data sources are updated instantaneously or "as often as every 15 minutes."[14] Beyond the U.S., it advertises data on individuals in dozens of countries including from "Citizen or National Database information, Credit Header File Information, Electoral Rolls, Property Records, Utility Data and Marketing Sources."[15] LexisNexis advertises a capability to identify active duty military personnel.[16] It also advertises a Phone Ownership Identification service that "combines robust phone and consumer content with industry-leading identity, relationship and association linking to determine every possible connection between the consumer and phone number provided."[17]



Advertisement of LexisNexis' SmartLinx Person Report. August 2021.

Nielsen: Nielsen broadly advertises audience data "across more than 60,000 segments," including demographics, psychographics, mobile, online, TV, over-the-top TV and audio behavior, spending, store visits, basket size, and product purchases.[18] It advertises purchase history across over 90 million households, in-store purchase data from over 18,000 retail and drug stores, and data from over 2.2 million Universal Product Codes, forming "the largest and most representative [Consumer Packaged Goods] buyer graphic dataset in the U.S."[19] It advertises data on online and offline transactions across MasterCard, Visa, Discover, and American Express, among others, "representing 80% of all credit card and 30% of all debit card transactions."[20] It also advertises a personality survey on individuals.[21] It advertises more than 400 data providers—including from Consumer Packaged Goods, travel, shopping, auto, finance, and business-to-business firms—in its Nielsen Marketing Cloud Data-as-a-Service platform.[22] Nielsen also explicitly advertises data on current and former U.S. military personnel. It published a report in 2019 on "today's veteran consumers" that drew on two external sources and four Nielsen data sets, attempting to depict what active and former U.S. military personnel watch, where veterans shop, what veterans spend on what they buy, and how that compares to what the average household buys.[23] Nielsen also advertises its "HomeScan DeCa (Defense Commissary Agency) database" which "tracks consumer

spending at military commissaries and exchanges."[24] The company has publicly published multiple other analyses of U.S. military personnel economic activity that draw on multiple Nielsen surveys and data sets.[25]

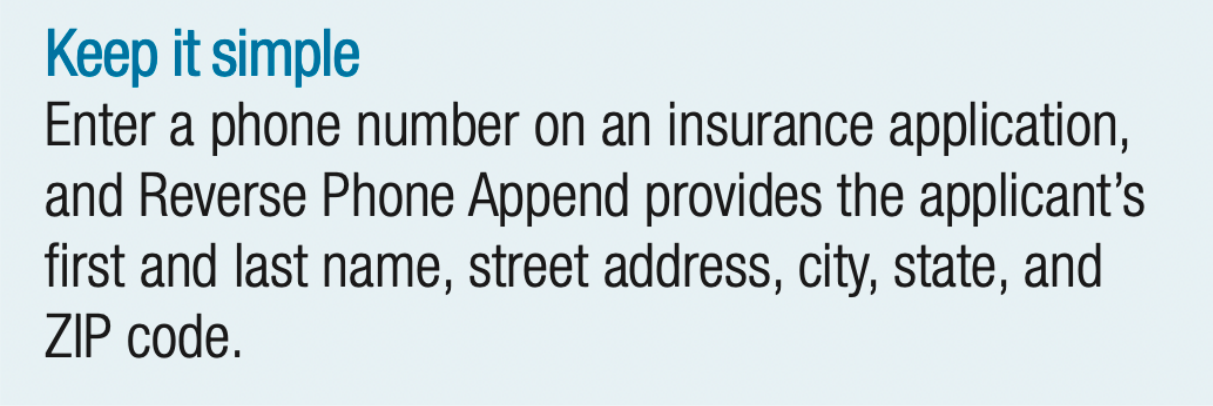
Experian: Experian says it processes over 2 billion records monthly and has over 8 billion name and address combinations, with the ability "to convert sensitive PII [personally identifiable information] data into actionable insights."[26] Experian advertises data on 95% of the U.S. population, including information on 300 million consumers, 126 million living units, and 4.4 billion economic transactions[27] spanning thousands of data attributes.[28] Experian advertises its ability to "ingest first-party data" such as names, physical addresses, email addresses, mobile ad identifiers (MAIDs), IP addresses, and other information to link economic transactions to "an Experian household ID."[29] It advertises mobile location data on users[30] and the ability to link information to 500 million email addresses and 275 million addressable cookies.[31] The company also advertises services to target individuals using first-party, second-party, or third-party data (terms not defined explicitly on the Experian website, but which likely refer to data a business directly collects on its users (first-party) versus that acquired indirectly (second- and third-party)).[32]

Equifax: Equifax advertises data on 45% of the nation's assets[33] spanning "digital targeting segments" including wealth, financial durability, auto, income, credit card spending propensities, business to business, mortgage, financial mobility, online interest, financial cohorts, investments, insurance, credit card, student loan, retail banking, small business assets, restaurant, ability to pay, communications, travel and leisure, sports, and more.[34] It advertises a service for clients to upload their own data on customers, after which Equifax can link the data with its own third-party data for insights.[35] It makes claims in multiple marketing documents about "anonymous" data, such as household wealth estimates, but it does not fully elaborate on how "anonymous" is defined nor when anonymization supposedly takes place.[36] Journalists have documented how Equifax purchases payroll and employee data from thousands of U.S. businesses;[37] Intuit, for instance, recently began sharing the payroll data of 1.4 million businesses with Equifax.[38]

CoreLogic: CoreLogic advertises data on "more than 99.99% of all properties in the United States."[39] It says that this includes over 1 billion property records sourced and updated annually,[40] as well as data on property listings, tax records, home valuations, and data related to properties including neighborhoods, flooding, and school data.[41] It says 99.75% of its data "is collected directly from the source."[42]

Verisk: Verisk advertises over 22 billion records in commercial and personal lines, "detailed information" on over 6 million commercial properties, insurance fraud data on over 1.4 billion claims, and "depersonalized information" on over 1.8 billion consumer credit, debit, and savings accounts.[43] It advertises its "Verisk Data Exchange" that has personal and commercial auto data, connected home data, and claims data, including from auto-makers (Ford, GM, Honda, and Hyundai are listed), telematics service providers (dongles, hardwired aftermarket devices, smartphones, and companies Omnitracs and TomTom are listed), mobile telematics providers, and connected home providers.[44] For example, it advertises data from over 3.5 million vehicles and on 43 billion miles of driving in its Verisk Data

Exchange.[45] Verisk identifies several potential sources of smart-home device data for its Data Exchange (though does not specify which are used), including video doorbells, security or surveillance cameras, motion detectors, window/door sensors, flow detectors, water shut-off valves, connected thermostats and temperature sensors, smoke detectors, air particulate detectors, fire detectors, smart appliances and plugs, and electrical panel monitors.[46] Verisk also advertises a "Reverse Phone Append" feature to get data on an individual "simply by entering their phone number."[47]



Advertisement of Verisk's "Reverse Phone Append" service. July 2021.

Oracle: Oracle advertises partnerships with over 74 other data providers accessible to clients through the Oracle BlueKai marketplace.[48] For example, Affinity Answers, one of the partner data providers, advertises data on billions of consumer engagements.[49] Affinity Answers advertises data on individuals' preferred stores, e-commerce websites, video streaming sites, internet service providers, cellular service providers, consumer products, television shows, podcast genres, sports teams, travel vendors (airlines, cruises, car rental services, etc.), and financial service firms (spanning banking and insurance). Affinity Answers also advertises data on individuals' interests in political organizations (e.g., NAACP, National LGBTQ Task Force, Planned Parenthood), political media figures (e.g., Bill O'Reilly, Glenn Beck, Anderson Cooper, Arianna Huffington), state-level Democratic Party and Republican Party organizations, and specific politicians in office.[50] Oracle has also purchased many data broker firms, such as Bluekai and Datalogix in 2014; at the time of purchase, Datalogix advertised data from 1,500 "data partners" that covered $2 trillion in consumer spending across 110 million households.[51] Oracle does not explicitly advertise data on current or former U.S. military personnel, but it provides data from Acxiom through its Oracle BlueKai marketplace, and Acxiom explicitly advertises data on U.S. military personnel (see above).

Epsilon: Epsilon advertises "vital data" on 250 million U.S. consumers, composed of over 7,000 attributes on each consumer, including transaction data and online behavior.[52] It also advertises millions of cross-device IDs.[53] It advertises its "Abacus Alliance," which it calls "the largest cooperative database in the U.S.," where more than 3,000 companies contribute data on individuals;[54] every week, Epsilon says, over 250 "multi-channel brands" upload customer transactional data, including what individuals purchased, when, where, and for

how much money.[55] It advertises sourcing records from public records (including voter registration files, phone books, deeds, and permits), surveys ("self-reported data from 20 million households"), partners (data from corporate sources), and "multi-sourced" information, which it describes as "real transactional data" on categories of purchases.[56]

Other—People-Search Websites: "People-search websites," commonly referred to as "white pages" websites, allow internet users to search for information on an individual by entering their name. These websites typically scrape this information from public records (property records, tax filings, voting records, etc.), aggregate it, and publish it online in a searchable format; these searches may be free-of-charge or run for a small fee. People-search websites cover much of the U.S. population, and as such, it is highly likely that, for example, many active and former U.S. military personnel's address, contact, and family information is searchable via these publicly available websites. The author was able to conduct searches on multiple, unnamed, publicly accessible people-search websites that appeared to provide data (e.g., phone numbers, address information) for senior members of the U.S. military. The same could be done for any number of activists or other individuals who are at higher risk of being targeted with violence by domestic organizations.

Analysis of Policy Implications for the United States

Threats to Civil Rights:

U.S. federal agencies from the Federal Bureau of Investigation (FBI) to U.S. Immigration and Customs Enforcement (ICE) purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations.[57] In doing so, data broker companies circumvent limits on companies directly handing data to law enforcement (e.g., a cellular company can sell user data to a data broker which can then sell the data to the FBI). The federal government agencies using the data may then also circumvent a variety of legal restrictions in place around searches and seizures as well as federal controls which are not applied to "open source" or "commercially obtained" data, even if the data is on U.S. individuals.

Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals' civil rights. Even if data brokers do not explicitly advertise these types of data (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make "predictions" or "inferences" about this kind of sensitive information (race, gender, sexual orientation, etc.) on individuals.[58]

This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements.[59] Many industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services. A 2018 ProPublica investigation, for example, found that health insurers were purchasing data from data brokers (including data on individuals' race, marital status, education level, net worth, TV consumption, and whether bills are paid on time) to predict health costs.[60] Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups. Data on military personnel has also been used for exploitative commercial purposes, as with for-profit schools using acquired data to target predatory advertisements or outright scams to veterans looking for educational opportunities.[61]

Companies are not required to inform individuals that they are being micro-targeted with advertisements using this data. Consumers do not necessarily know that the data about them is being collected; nor in most cases do they have legal recourse to have the data corrected by a data broker if it is inaccurate (e.g., incorrectly logging a felony conviction).[62] The last of these possibilities is not hypothetical: a 2020 investigation by The Markup identified dozens of cases in which Americans were denied housing because of mistakes in criminal record data—data which the companies in question often acquired from data brokers or people-search websites.[63]

Data brokers' troves of data on U.S. individuals also pose threats to civil rights from the government side. Given a long history of American law enforcement exclusively or disproportionately targeting marginalized individuals and communities with surveillance,[64] there is also great risk that data points on individuals' race, ethnicity, gender, sexual orientation, immigration status, and other demographic characteristics will be used in discriminatory policing and surveillance. This data could also be acquired, without a warrant, for law enforcement use in training artificial intelligence surveillance tools. It could also be outright wrong: a 2019 ruling by a U.S. district court in California found that "[t]he databases on which ICE relies for information on citizenship and immigration status often contain incomplete data, significant errors, or were not designed to provide information that would be used to determine a person's removability."[65]

Data brokers could also be hacked—especially where data brokers do not adequately invest in cybersecurity—and sensitive data on U.S. individuals could be publicly leaked in damaging ways. For example, data broker Social Data in 2020 was found to have an unsecured, non-password-protected database facing the public internet with data on 235 million social media profiles, all due to a database configuration error.[66]

And individuals can use this data held by data brokers to discriminate against others as well. The Catholic website The Pillar recently outed a gay priest by purchasing data on the individual's Grindr usage (including location data) from a third party that obtained it from the app.[67] This will not be the last time an individual's location data was acquired by a third party intent on inflicting harm. Members of vulnerable communities may not be aware that their data is widely collected, aggregated, and sold to whomever is buying, such as with LGBTQ individuals using dating apps and sharing their GPS location, sexual preferences, sexual health statuses, and more. Research from Duke's Cyber Policy and Gender Violence Initiative has also identified numerous ways in which abusive individuals can use people-search websites to obtain data broker data to carry out stalking, harassment, and physical violence against intimate partners—violence which is overwhelmingly directed at women and members of the LGBTQ community.[68] Privacy is quite literally, as the Cyber Policy and Gender Violence Initiative says, a matter of life and death for survivors of domestic violence, yet data broker websites can publish and sell information on an individual's address with no restrictions. Individuals could similarly obtain information about activists, political organizers, and other people for the purposes of violence, intimidation, or harassment as well.

Threats to National Security:

Three of the 10 data brokers surveyed for this report—Acxiom, LexisNexis, and Nielsen—openly and explicitly advertise data on current and/or former U.S. military personnel. LexisNexis identifies a capability to specifically identify active U.S. military personnel. Data sets on U.S. military personnel are not necessarily used for nefarious purposes: current and former U.S. military personnel are a unique demographic, and as such, many different industries may want to target them with uniquely tailored advertisements for products and services. It is also possible some data brokers may offer economic opportunities through the

use of this information without actually selling the information to a client—e.g., allowing a client insurance firm to run ads through the data broker's platform, but without ever handing over the underlying data on particular individuals.

That said, many data brokers actively sell their data sets to willing buyers. There is little transparency, if any at all, into data brokerage transactions. There is also virtually nothing in U.S. law preventing data brokers from selling information on U.S. individuals to foreign entities. The data advertised by these brokers—spanning everything from financial transaction histories and internet browsing patterns to travel interests and support for political causes and organizations—could be used by foreign entities for a range of national security-damaging activities. This could include building profiles on senior U.S. military personnel involved in key decisions relevant to a foreign power, or even building profiles on their family members and close acquaintances (seeing as some data brokers openly and explicitly advertise their ability to map network connections between individuals), for the purposes of information operations, coercion, blackmail, or intelligence-gathering. Should terrorist organizations acquire any of this data broker data on U.S. military personnel, the consequences could potentially even be more dire. As mentioned, there are few mechanisms in place for the U.S. government to limit the sharing of data brokerage data, including highly sensitive data, on U.S. individuals. Buyers of data broker data could potentially combine data from multiple brokers together to, for example, uncover a U.S. military or government employee's family member and then obtain their real-time location and/or location history.

More broadly, the data on U.S. individuals held by data brokers is highly sensitive and could be used in many other ways to undermine U.S. national security. Foreign actors, such as Russia's Internet Research Agency, could use this data to bolster their influence campaigns to interfere in U.S. electoral processes. Criminal organizations could use this data to build profiles on and subsequently target prosecutors and judges. Foreign intelligence organizations could acquire this data through a variety of means—including through front companies that could legally purchase the data from U.S. brokers, and through simply hacking a data broker and stealing it all—to build profiles on politicians, media figures, diplomats, civil servants, and even suspected or secretly identified intelligence operatives.

Threats to Democracy:

Data on U.S. individuals shared and/or sold by U.S. data brokers could be used for activities that specifically threaten elements of the U.S. democratic electoral system, such as by foreign governments micro-targeting individuals with election disinformation intended to sow chaos or dissuade voter participation (e.g., as the Russian Internet Research Agency did to Black communities in 2016)[69] or by domestic terror organizations carrying out voter intimidation and suppression. For example, there is virtually nothing in U.S. law preventing data brokers from selling highly sensitive political preference information on millions of U.S. individuals to foreign entities. Political campaigns in the United States already purchase data broker data to plan and execute their outreach to U.S. voters, though voters have little visibility into the details of this practice.[70]

Broadly, the data brokerage ecosystem represents the unrestrained aggregation of surveillance power as a service. Companies openly and explicitly advertise immense data sets on U.S. individuals with thousands of sub-attributes that reveal highly sensitive behavior—from marketing materials that detail information on individuals' economic activity and health provider preferences to a company advertising a tool to search anyone's phone number and return a name, address, and other information (which can then be used for subsequent data-searching). Federal law enforcement agencies purchase information from data brokers in a manner that has the impact of circumventing protections against acquiring and using data on U.S. individuals; companies use data brokers to develop "predictive" models on consumers and to discriminately target goods and services; and individuals are increasingly using data brokers to inflict harm on vulnerable communities and specific other individuals. Entities that purchase or otherwise acquire data from multiple brokers—again, a practice that is virtually unregulated in the United States—would have an even larger, more intimate, and consequently more dangerous data set. The purchasing of detailed data sets on military personnel is an illustrative example of business practices that do not have sufficient oversight or accountability.

Conclusion:

There are virtually no controls on the data brokerage industry (data broker firms specifically) and on the practice of data brokerage itself (the broader buying, licensing, and sharing of data that underpins these companies' operation). Americans also do not have federal privacy rights to gain insight into the data brokerage ecosystem's surveillance of them, nor do they have federal rights to demand that incorrect data is corrected;[71] federal enforcement agencies like the Federal Trade Commission, conversely, do not have a strong federal privacy law to point to as grounds to investigate unfair and exploitative practices by data brokers and by firms using data broker data. All these harms—to Americans' civil rights, to U.S. national security, and to U.S. democracy writ large—will only persist without further regulation.

Endnotes

[1] For complete disclosure of funders of the Duke University Sanford Cyber Policy Program, see the External Relationships section of https://scholars.duke.edu/person/David.Hoffman. No specific direct funding was provided for this report, and no funders reviewed any of this research before publication or had any editorial control over the report's substantive content.
[2] Justin Sherman, "Federal Privacy Rules Must Get 'Data Broker' Definitions Right," *Lawfare*, April 8, 2021, https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right.
[3] Acxiom, *Global Data Navigator*, https://www.acxiom.com/wp-content/uploads/2018/03/Fact_Sheet_Global_Data_Navigator.pdf, 2.
[4] Acxiom, *InfoBase*, https://www.acxiom.com/wp-content/uploads/2020/07/ac-2490-19-fs-acxiom-infobase.pdf, 1.
[5] Ibid., 2.
[6] Acxiom, *Gated Offers*, https://www.acxiom.com/wp-content/uploads/2020/07/AC-0991-20_Collateral_Fact_Sheet_Gated_Offers_-_GENERIC_Final_5-19-20.pdf.
[7] Acxiom, *Government Capability Statement*, https://www.acxiom.com/wp-content/uploads/2019/11/government-capability-statement-fact-sheet-9-24-19.pdf, 2.
[8] LexisNexis, "Our Technology," Risk.LexisNexis.com, https://risk.lexisnexis.com/our-technology; LexisNexis, "Public Records," Risk.LexisNexis.com, https://www.lexisnexis.com/en-us/products/public-records.page.
[9] LexisNexis, "Search Public Records," Risk.LexisNexis.com, https://www.lexisnexis.com/en-us/products/public-records/powerful-public-records-search.page.
[10] Ibid.
[11] LexisNexis, "Up to 1 million new records daily," Risk.LexisNexis.com, https://www.lexisnexis.com/en-us/products/public-records/dynamic-continuously-updated-collection.page.
[12] LexisNexis, "Crime and Criminal Investigation Solutions," Risk.LexisNexis.com, https://risk.lexisnexis.com/law-enforcement-and-public-safety/crime-and-criminal-investigations.
[13] Ibid.
[14] LexisNexis, "Law Enforcement Data, Analytics & ID Linking," Risk.LexisNexis.com, https://risk.lexisnexis.com/law-enforcement-and-public-safety.
[15] LexisNexis, "Instant Verify International," Risk.LexisNexis.com, https://risk.lexisnexis.com/global/en/products/instant-verify-intl-global.
[16] LexisNexis, "Collections Compliance," Risk.LexisNexis.com, https://risk.lexisnexis.com/collections-and-recovery/collections-compliance.
[17] Ibid.
[18] Nielsen, "Nielsen Data As a Service," Nielsen.com, https://www.nielsen.com/us/en/solutions/capabilities/nielsenmarketingcloud-daas/.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Nielsen, *Beyond the Uniform*, https://www.nielsen.com/wp-content/uploads/sites/3/2019/07/beyond-the-uniform-a-look-at-todays-veteran-consumers.pdf.
[24] Nielsen, "Serving Today's Military Consumers," Nielsen.com, November 4, 2014, https://www.nielsen.com/us/en/insights/article/2014/serving-todays-military-consumers/.
[25] See, e.g., Nielsen, "Connecting with Women in the Military," Nielsen.com, May 17, 2016, https://www.nielsen.com/us/en/insights/article/2016/connecting-with-women-in-the-military/; Nielsen, "Roger That: Reaching Today's Military Consumers," Nielsen.com, November 10, 2014, https://www.nielsen.com/us/en/insights/article/2014/roger-that-reaching-todays-military-consumers/.
[26] Experian, "OmniView," Experian.com, accessed July 2020, https://www.experian.com/marketing-services/omniview.
[27] Experian, *ConsumerView: Data by the Numbers*, https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/infographics/consumerview.pdf.

[28] Experian, *ConsumerView*, https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/brochures/consumerview-brochure.pdf, 3.
[29] Experian, *OmniImpact*, https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/product-sheets/omniimpact.pdf, 1.
[30] Ibid.
[31] Experian, *ConsumerView: Data by the Numbers.*
[32] Experian, *ConsumerView*, 8.
[33] Equifax, "Why Equifax?" DataDrivenMarketing.Equifax.com, https://datadrivenmarketing.equifax.com/why-equifax/overview/.
[34] Equifax, "Digital Targeting Segments," DataDrivenMarketing.Equifax.com, https://datadrivenmarketing.equifax.com/digital-targeting-segments/.
[35] Equifax, "Overview of Services," DataDrivenMarketing.Equifax.com, https://datadrivenmarketing.equifax.com/capabilities/overview/.
[36] See, e.g., Equifax, *WealthComplete Household Direct Digital*, URL, 3; Equifax, *Digital Targeting Segments: Online Interest*, https://resources.datadrivenmarketing.equifax.com/digital-marketing/digital-targeting-segments-online-interest?_ga=2.222403995.1491988852.1625766298-1515325844.1625671484, 1, 2.
[37] Jennifer Surane, "Equifax Amassed Salary Details for People at 7,100 Companies," *Bloomberg*, October 2, 2017, https://www.bloomberg.com/news/articles/2017-10-02/equifax-has-amassed-salary-details-for-people-at-7-100-companies.
[38] Brian Krebs, "Intuit to Share Payroll Data from 1.4M Small Businesses With Equifax," Krebs on Security, July 1, 2021, https://krebsonsecurity.com/2021/07/intuit-to-share-payroll-data-from-1-4m-small-businesses-with-equifax/.
[39] CoreLogic, "Property Data Solutions," CoreLogic.com, https://www.corelogic.com/find/property-data-solutions/.
[40] CoreLogic, "Gold Standard Data & Property Solutions," CoreLogic.com, https://www.corelogic.com/why-corelogic/.
[41] CoreLogic, "The Benefits of Trestle" (video) on "Trestle," Trestle.CoreLogic.com, https://trestle.corelogic.com/Home/AssertionConsumer/Brokers.
[42] CoreLogic, "Gold Standard Data."
[43] Verisk, "Verisk Analytics Fact Sheet," Verisk.com, https://www.verisk.com/verisk-in-the-news/verisk-analytics-fact-sheet/.
[44] Verisk, "The Verisk Data Exchange," Verisk.com, https://www.verisk.com/insurance/products/telematics/.
[45] Saurabh Khemka, "Omnitracs to join Verisk Data Exchange," Verisk.com, June 14, 2018, https://www.verisk.com/insurance/visualize/omnitracs-to-join-verisk-data-exchange/.
[46] Sandra Maples, "How smart devices are providing the data claims professionals need," Verisk.com, October 3, 2017, https://www.verisk.com/insurance/visualize/how-smart-devices-are-providing-the-data-claims-professionals-need/.
[47] Verisk, "Reverse Phone Append," Verisk.com, https://www.verisk.com/insurance/products/reverse-phone-append/.
[48] "Oracle Audiences," Oracle.com, https://www.oracle.com/cx/advertising/audiences/; "Branded Data Providers," Oracle.com, https://www.oracle.com/cx/advertising/data-providers/.
[49] "Social Insights-Powered Audiences," AffinityAnswers.com, https://www.affinityanswers.com/programmatic-display/.
[50] Affinity Answers Syndicated Taxonomy, June 2020 (Excel file), downloaded from "Social Insights-Powered Audiences."
[51] "Oracle Buys Datalogix," Oracle.com, December 22, 2014, https://www.oracle.com/corporate/pressrelease/oracle-buys-datalogix-122214.html.
[52] "Understand your customer analytics with consumer data," Epsilon.com, https://www.epsilon.com/us/products-and-services/data; "Financial Services Digital Marketing Solutions," Epsilon.com, https://www.epsilon.com/us/industries/financial-services.
[53] "Power of Me," Epsilon.com, https://us.epsilon.com/power-of-me.
[54] "Understand your customer analytics."
[55] "Direct mail success with Epsilon's Abacus Alliance," Epsilon.com, https://www.epsilon.com/abacus/the-abacus-alliance.

[56] "Do more with your data to drive better outcomes," Epsilon.com, https://www.epsilon.com/us/products-and-services/data.
[57] See, e.g., Sara Morrison, "A surprising number of government agencies buy cellphone location data. Lawmakers want to know why," *Recode*, December 2, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; Joseph Cox, "CBP Bought 'Global' Location Data from Weather and Game Apps," *VICE*, October 6, 2020, https://www.vice.com/en/article/n7wakg/cbp-dhs-location-data-venntel-apps; Drew Harwell, "ICE investigators used a private utility database covering millions to pursue immigration violations," *The Washington Post*, February 26, 2021, https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/.
[58] See, e.g., among many others, Thorin Klosowski, "Big Companies Harvest Our Data. This Is Who They Think I Am," *The New York Times*, May 28, 2020, https://www.nytimes.com/wirecutter/blog/data-harvesting-by-companies/; "Data Brokers: A Call for Transparency and Accountability," Statement of Commissioner Julie Brill, Federal Trade Commission, May 27, 2014, https://www.ftc.gov/system/files/documents/public_statements/311551/140527databrokerrptbrillstmt.pdf.
[59] This was the subject of a U.S. Department of Housing and Urban Development complaint in 2018: "US regulators target Facebook on discriminatory housing ads," Associated Press, August 17, 2018, https://apnews.com/article/north-america-lawsuits-us-news-real-estate-brokers-tx-state-wire-f02eb72214ac43638ba1a5ab6daea4e8. A July 2021 investigation by *The Markup* found that Facebook still uses many proxies for categories like race in its advertising tools: Jon Keegan, "Facebook Got Rid of Racial Ad Categories. Or Did It?" *The Markup*, July 9, 2021, https://themarkup.org/citizen-browser/2021/07/09/facebook-got-rid-of-racial-ad-categories-or-did-it.
[60] Marshall Allen, "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates," ProPublica, July 17, 2018, https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.
[61] See, e.g., *Private For-Profit Colleges and Online Lead Generation* (Washington, D.C.: Center for Digital Democracy, May 2015), https://www.democraticmedia.org/sites/default/files/field/public-files/2015/forprofitcollegeleadgenreport_may2015_uspirgef_cdd_0.pdf; "The Predatory Underworld of Companies that Target Veterans for a Buck," Student Borrower Protection Center, https://protectborrowers.org/the-predatory-underworld-of-companies-that-target-veterans-for-a-buck/.
[62] Fair Credit Reporting Act protections are an exception, but the individual's rights are limited to just specific uses of the data by the data broker.
[63] Lauren Kirchner, "When Zombie Data Costs You a Home," The Markup, October 6, 2020, https://themarkup.org/locked-out/2020/10/06/zombie-criminal-records-housing-background-checks.
[64] See, e.g., Alvaro Bedoya, "The Color of Surveillance," *Slate* Magazine, January 28, 2016, https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html; Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015).
[65] Joan Friedland, "How the Trump Deportation Machine Relies on Inaccurate Databases and Unregulated Data Collection," National Immigration Law Center, November 1, 2019, https://www.nilc.org/2019/11/01/inaccurate-data-unregulated-collection-fuel-deportation-machine/.
[66] Scott Ikeda, "Major Data Broker Exposes 235 Million Social Media Profiles in Data Leak," *CPO Magazine*, August 28, 2020, https://www.cpomagazine.com/cyber-security/major-data-broker-exposes-235-million-social-media-profiles-in-data-leak/.
[67] "Priest outed via Grindr app highlights rampant data tracking," NBC News, July 22, 2021, https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493.
[68] "Privacy Issues from Data Brokers," Duke Cyber Policy and Gender Violence Initiative, https://sites.sanford.duke.edu/genderviolencepolicy/privacy-issues-for-gender-violence-survivors/; "Domestic Violence and the LGBTQ Community," National Coalition Against Domestic Violence, June 6, 2018, https://ncadv.org/blog/posts/domestic-violence-and-the-lgbtq-community.
[69] Jason Parham, "Targeting Black Americans, Russia's IRA Exploited Racial Wounds," *WIRED*, December 17, 2018, https://www.wired.com/story/russia-ira-target-black-americans/.
[70] Geoffrey A. Fowler, "How politicians target you: 3,000 data points on every voter, including your phone number," *The Washington Post*, October 27, 2020,

https://www.washingtonpost.com/technology/2020/10/27/political-campaign-data-targeting/; Jeremy B. Merrill, "How to Wrestle Your Data From Data Brokers, Silicon Valley — and Cambridge Analytica," ProPublica, April 30, 2018, https://www.propublica.org/article/how-to-wrestle-your-data-from-data-brokers-silicon-valley-and-cambridge-analytica.

[71] Some narrow rights may apply with respect to certain categories of data, such as children's data or clinical health data, or data uses, such as credit reporting.