DATA BROKERS: A BENEFIT OR PERIL TO U.S. NATIONAL SECURITY?

STEVEN JOSEPH ARANGO*

Do you know what data exists about you? Do you know what data you create . . . every second of the day? Probably not. But data brokers do. At first glance, this may make you uncomfortable. But with deeper analysis, it should make you downright concerned. Data brokers sell information about you, ranging from addictions to diseases to who you slept with. In other words, information you likely wouldn’t share with your friends is for sale.

And the U.S. Government and its foreign adversaries (think Iran and China) can buy it—legally. Under the current U.S. regulatory and legal landscape, there is little stopping the U.S. Government or its adversaries from doing so. This data is a goldmine for intelligence operations, but its sale also raises serious privacy concerns that must not be ignored.

To address these topics, this paper will first explain the technical background necessary to understand data brokers and how they connect this data to individuals—including you. In the following sections, the paper lays out the perils and benefits that data brokers pose to U.S. national security, the regulatory landscape for data broker sales, and the privacy concerns for American citizens created by these sales. With these foundational points explained, the paper concludes with recommendations on how to best protect U.S. national security without eroding America’s bedrock civil liberties.

* Captain Steven Arango, USMC, is a deputy staff judge advocate at Training and Education Command and currently working toward his LL.M. in national security and cybersecurity from the George Washington University School of Law. The views expressed in this article are those of the author and do not necessarily represent the views of the U.S. Marine Corps, Dep’t of the Navy, Dep’t of Defense, or the U.S. Government. He dedicates this paper to his son, Milo Arango, and his wife, Captain Rebecca Arango, USAF. Without them, this paper would not have been possible.
I. INTRODUCTION .................................................................................. 109
II. TECHNICAL BACKGROUND .............................................................. 111
   A. Data Brokers ........................................................................... 111
   B. Identifiers .............................................................................. 114
III. DATA BROKERS AND NATIONAL SECURITY .............................. 119
   A. National Security Perils ......................................................... 120
   B. National Security Benefits ..................................................... 122
IV. ASSESSMENT OF THE REGULATORY LANDSCAPE ...................... 124
   A. Self-Regulation ...................................................................... 125
   B. Consent by User ..................................................................... 127
   C. FTC Regulation ....................................................................... 128
   D. Legislative ............................................................................ 130
V. PRIVACY ISSUES FOR U.S. CITIZENS ........................................... 131
VI. WAY FORWARD ............................................................................... 133
   A. Foreign Adversaries ................................................................. 133
   B. U.S. Government ..................................................................... 135
VII. CONCLUSION .................................................................................. 137
I. INTRODUCTION

China can legally purchase almost every important detail about your life.1 So can Russia.2 Iran too.3 Because of data brokers, U.S. foreign adversaries can purchase vast amounts of information on U.S. citizens, such as location data, purchase history, and web browsing.5 They can establish where you are, your pattern of life, and if they deem you important enough, find a way to target you.6 Without spending a dime on traditional espionage, such as signals intelligence or human intelligence, foreign adversaries can accomplish their national security objectives. In fact, “[foreign adversaries] can buy data from such brokers on thousands or even millions of Americans for less than the price of a new suit.”7 But within every peril lies a potential benefit: the U.S. Government can also use data brokers to improve its national security.8 To make matters more complicated, tangled in this national security web are U.S. citizens’ privacy concerns.9

Without the “modern surveillance economy”, there would be no

---

2 Littell et al., supra note 1.
3 Id.
4 Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 9, 2021). For this paper, “the term ‘foreign adversary’ means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.”
5 Wyden, supra note 1.
6 Littell et al., supra note 1; Wyden, supra note 1.
7 Trevor Logan & Theo Lebryk, The United States Has a Data Broker Problem, FOUND. FOR DEF. OF DEMOCRACIES (May 13, 2021), https://www.fdd.org/analysis/2021/05/13/the-united-states-has-a-data-broker-problem/ [https://perma.cc/FQ75-YG9C].
data brokers.\textsuperscript{10} This economy is made up of thousands of companies from various industries that collect, analyze, acquire, share, trade, and utilize data on billions of people.\textsuperscript{11} The companies involved are widespread, ranging from financial institutions to tech companies to auto manufacturers.\textsuperscript{12} The economy keeps growing too—more and more companies seek to join as they develop more devices and apps that collect data.\textsuperscript{13}

Data brokers feed off this economy. They want to know everything about you—without your explicit knowledge or consent—to monetize your data, turning it from unrelated pieces of data into a multi-billion dollar industry (upwards of $200 billion).\textsuperscript{14} They sell information about you varying from addictions to genetic diseases to where you work and live.\textsuperscript{15} There is little to no U.S. federal regulation or laws governing the data broker industry and no governing who they can sell to.\textsuperscript{16} As a result, data brokers have an unlimited ability to sell their data to who they want.

Data, including data from data brokers, has undercut the business of espionage.\textsuperscript{17} Advancements in data collection have shaken the two foundations of spying: “people pretending to be someone who they are not and operating in the shadows.”\textsuperscript{18} In the intelligence community, the U.S. wants to increase its ability in both realms.\textsuperscript{19} However, data has made doing so difficult, requiring increased

\begin{flushright}
\textsuperscript{10} Littell et al., supra note 1.
\textsuperscript{11} WOLFIE CHRISTL, CORPORATE SURVEILLANCE IN EVERYDAY LIFE 4 (2017).
\textsuperscript{12} BENNETT CYPHERS & Gennie Gebhart, BEHIND THE ONE-WAY MIRROR: A DEEP DIVE INTO THE TECHNOLOGY OF CORPORATE SURVEILLANCE 31 (2019).
\textsuperscript{14} Laura Palk & Krishnamurty Muralidhar, A Free Ride: Data Brokers’ Rent-Seeking Behavior and the Future of Data Inequality, 20 VAND. J. ENT. & TECH. L. 779, 820–21 (2018); CHRISTL, supra note 11, at 4.
\textsuperscript{17} Telephone Interview with Duyane Norman, Retired Member, CIA Senior Intel. Serv. (Mar. 22, 2023).
\textsuperscript{18} Id.
\textsuperscript{19} Id.
\end{flushright}
resources with a “[disproportionate] rate of return.” One must ask: can anything be done or is this data-enriched world one the U.S. Government must learn to operate in?

This paper will first address the technical background necessary to understand data brokers and how they connect this data to individuals—including you. In the following sections, the paper lays out the perils and benefits that data brokers pose to U.S. national security, the regulatory landscape for data broker sales, and the privacy concerns for U.S. citizens created by these sales. With these foundational points explained, the paper concludes with recommendations on how to best protect U.S. national security without eroding America’s bedrock civil liberties.

II. TECHNICAL BACKGROUND

A. Data Brokers

One must properly define data brokers to understand and legislate them. Some define data brokers as “companies that sell information about individuals with whom they have no direct business relationship.” Naturally excluded from this definition are companies that sell data about its customers. The Federal Trade Commission (FTC) defines data brokers as “companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual’s identity, or detecting fraud.” The Sanford School of Public Policy at Duke University defines data brokers as companies that broker data. Under this definition, the relationship with consumers matters not—simply the fact that data is exchanged.

---

20 Id.
23 Id.
25 Sherman et al., supra note 22, at 5.
26 Id.
This lack of consensus creates patchwork approaches that do not adequately address the data broker issue.

The Sanford definition should be used and applies throughout this paper. Using a more limited definition, such as the one that requires “no direct business relationship”, creates undesirable results. For example, one data broker, Life360, “was secretly selling precise location data on its parent and child users and in 2020 made almost 20 percent of its revenue from this brokerage.” Under the limited definition, Life360 would not be a data broker because the company had a direct business relationship with the consumer—even though the end result is the same. At bottom, the data is what matters, not the relationship.

Data brokers—without the express consent or knowledge of a consumer—collect billions of data points on U.S. citizens from public and non-public sources. Public sources often are publicly available records or information online. Non-public sources are mainly from private companies, where data emanates from places such as smart devices, applications, or browsing history. For instance, there are applications that test blood sugar, record how you sleep, and monitor blood pressure; other apps require biometric information (e.g., your face) to use the app. Regardless of the product, all these apps create data points, which data brokers collect. Data brokers also stockpile data on your communications, finances, sexual orientation, health, addresses, location, and many other sensitive areas of your life.

Data brokers package data in different manners. Some buy and

\[\text{27} \text{ See id.}\]
\[\text{28} \text{ Id. at 6.}\]
\[\text{29} \text{ Sherman, supra note 21.}\]
\[\text{30} \text{ Sherman et al., supra note 22, at 12; Kans, supra note 9; Palk & Muralidhar, supra note 14, at 984; Fed. Trade Comm’n, supra note 24, at 46.}\]
\[\text{31} \text{ Kans, supra note 9.}\]
\[\text{32} \text{ Id.}\]
sell raw data—a straight forward business model. Others will purchase data from numerous sources, then process and tailor the data for their specific customer. As part of these packages, some data brokers will use algorithms to infer traits about individuals, creating even larger profiles. These algorithms can determine intimate details about someone, ranging from sexual orientation to emotional stability and depression. Some data brokers will bundle data by specific groups, such as government employees and military status.

There are thousands of data brokers, but only two major data brokers will be highlighted here: Acxiom and Oracle. Acxiom’s clients stem from the Fortune 100 list, including healthcare, government, and telecommunications companies. Acxiom’s tentacles are far-reaching: they claim to have “data coverage of over 62 countries and the ability to reach over 2.5 billion consumers globally, [including] 45.5 million current and former U.S. military personnel.”

Oracle is one of the largest data brokers in the world. Oracle recently acquired numerous data companies to bolster their data broker services too. These companies collect data on a range of areas from purchases, activity data, and social media network messages. When Oracle cannot purchase the company, they rely on third-party data providers to help bolster their data pool. Two of their many third-party providers are VisualDNA and PlaceIQ. The former has “psychographic profiles on 500 million users in the U.S., U.K., Germany, Russia, and other [countries]”, the latter “collects location

36 Cyphers & Gebhart, supra note 12, at 39.
37 Id.; Fed. Trade Comm’n, supra note 24, at 22.
38 Christl., supra note 11, at 71.
39 Sherman et al., supra note 22, at 8.
40 Christl., supra note 11, at 41.
41 Id.
43 Christl., supra note 11, at 59.
44 Id.
45 Id.
46 Id.
47 Id.
48 Id.
data, movement patterns, and activity profiles from 100 million mobile devices.\textsuperscript{49}

![Table 1](image)

**Table 1**\textsuperscript{50}

B. Identifiers

Anonymization and pseudonymization are the two common methods for encrypting data.\textsuperscript{51} Even though these two methods are essential to encryption, they are often conflated.\textsuperscript{52} When data is anonymized, there is no longer the ability to identify individuals connected to that data.\textsuperscript{53} In contrast, pseudonymization removes “the immediate inference of the data subject from the data”, but one could still re-identify or unmask the subject by using other data sets.\textsuperscript{54} To illustrate, think of the game *Guess Who*. In the game, you have one person that you are trying to identify. Each turn, you can ask one question about the person’s identity (e.g., does the subject have glasses or is his hair color brown?). As you gain more information, you are able to identify the person. Unmasking someone works the same way: as more and more data points are collected, you can narrow down who those data points connect to.\textsuperscript{55} And because of the enormous amount of

\textsuperscript{49} Id.

\textsuperscript{50} This is an example of a data broker’s offerings and pricing sheet.

\textsuperscript{51} Interview with Johnathan Rudy, Senior Corp. Couns., TransUnion (Mar. 24, 2023).

\textsuperscript{52} Id.

\textsuperscript{53} Id.

\textsuperscript{54} Id.; CHRIStL, supra note 11, at 69.

\textsuperscript{55} CHRIStL, supra note 11, at 69; Boris Lubarsky, Re-Identification of “Anonymized” Data, 1 GEO. L. TECH. REV. 202, 203 (2017).
data and computing power that exists, it is “becoming increasingly difficult” to anonymize data—if not impossible.\textsuperscript{56}

Data brokers argue that their consumer data is anonymized—it is often not.\textsuperscript{57} To be sure, these companies “remove names and convert email addresses and phone numbers into unique alphanumeric string codes.”\textsuperscript{58} But this approach simply creates pseudonyms, allowing for unmasking.\textsuperscript{59} In fact, unmasking these individuals is an entire industry in of itself.\textsuperscript{60} “One recent study found that with only 15 specific demographic attributes, it would be possible to re-identify 99.98% of Americans in a dataset.”\textsuperscript{61} Data alone is valuable; data linked to devices and individuals is even more valuable.\textsuperscript{62} In other words, anonymity is bad for business.\textsuperscript{63}

Unmasking data can be done with ease too.\textsuperscript{64} In Professor Paul Ohm’s seminal work, he details three examples of “anonymization” gone awry.\textsuperscript{65} Each situation started with a company or agency releasing data that it thought it had anonymized—thus making it impossible to identify individuals linked to the data.\textsuperscript{66} They were wrong.\textsuperscript{67} In each case, people were able to unmask individuals “by discovering pockets of surprising uniqueness remaining in the data” and then combining that uniqueness with other data sets linked to individuals.\textsuperscript{68}

Companies use a multitude of identifiers to unmask a user such as cookies.\textsuperscript{69} Cookies “consist of text”, which are inserted in a user’s

\textsuperscript{56} Interview with Johnathan Rudy, \textit{supra} note 51; Paul Ohm, \textit{Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization}, 57 UCLA L. REV. 1701, 1716, 1730 (2010).
\textsuperscript{57} CHRISTL, \textit{supra} note 11, at 69.
\textsuperscript{58} Id.
\textsuperscript{59} Id.
\textsuperscript{61} Sherman et al., \textit{supra} note 22, at 10.
\textsuperscript{62} KIRSTEN HAZELRIG, INTELLIGENCE AFTER NEXT 3 (2023); Lubarsky, \textit{supra} note 55, at 203.
\textsuperscript{63} Sherman et al., \textit{supra} note 22, at 10. Unmasking someone is impossible; “aggregated data can still cause harm.” For example, figuring out traffic patterns for certain office locations or the attributes and weaknesses of people that work in a certain sector could be helpful to a foreign adversary.
\textsuperscript{64} Ohm, \textit{supra} note 56, at 1716.
\textsuperscript{65} Id.
\textsuperscript{66} Id. at 1723.
\textsuperscript{67} Id.
\textsuperscript{68} Id.
\textsuperscript{69} Sherman et al., \textit{supra} note 22, at 10; CYPHERS & GEBHART, \textit{supra} note 12, at 22.
browser and remain for review by a server. To illustrate, imagine a website. Different parts of this website are often “sourced from other domains.” One part may house advertisements; another may hold articles from across the internet. Each part can be and generally is established by third parties with access to the website. Because of this access, third parties can place their own cookies, called third-party cookies. The average user only sees and understands the URL (website link) that they input in the address bar—but a visit to this website, similar to others, pings “tens or hundreds of other servers” through these cookies. Although there are restrictions on what third parties can track, third parties have found loop holes to these restrictions, allowing them to circumvent these rules. So each time you visit a web browser, you create “several pieces of information that can be used to track you” by third parties, such as these cookies.

To be sure, not every cookie is meant to track individuals. For example, when you save your login and password for a specific website on your computer, cookies provide this option. Or when you place an item in a shopping cart on your favorite website, cookies allow you to do so. But cookies are mainly used for tracking purposes. Indeed, users have the ability to limit cookies—disabling third-party cookies at their request or blocking them through browser extensions. And to be clear, cookies per se are not a problem. Cookies have become a problem because data brokers, and in turn, foreign adversaries can purchase information collected by cookies and weaponize it.

Another identifier is an IP address. Your IP address is a “temporary identifier that’s unique to your device.” Each time you move to a network, a new IP address is generally created—e.g., you

71 Id. at 228.
72 Id.
73 Id.
74 Id.
75 Id.
76 Id. at 229.
77 CYPHERS & GEBHART, supra note 12, at 8.
78 Id.
79 Veale & Borgesius, supra note 70, at 227.
80 Id. at 241.
81 Id. at 227; CYPHERS & GEBHART, supra note 12, at 8.
82 CYPHERS & GEBHART, supra note 12, at 8.
83 Interview with Johnathan Rudy, supra note 51.
84 CYPHERS & GEBHART, supra note 12, at 13.
move from your house to a local coffee shop.\textsuperscript{85} Alone, IP addresses are a poor method to identify an individual; however, an IP address’ value lie in its ability to combine with other pieces of data to create “long-term profiles of users.”\textsuperscript{86} There are ways to block an IP address from third-party trackers, such as using a “VPN or the Tor browser.”\textsuperscript{87} But the average Internet user does not know how to use a VPN or Tor browser.

Mobile devices provide their own unique identifiers. When a device connects to a mobile network, it is “assigned a unique identifier called an International Mobile Subscriber Identity (IMSI) number.”\textsuperscript{88} Mobile carriers assign IMSIs, which are stored on the SIM card in the phone.\textsuperscript{89} Device owners cannot change the IMSI without changing the SIM card.\textsuperscript{90} Each time your phone pings a cell tower—which is constant—the unique IMSI populates with the cell provider.\textsuperscript{91} In other words, the IMSI is a personal location tracker. Even if you change the SIM card, each “mobile device has an International Mobile Equipment Identity (IMEI) number ‘baked’ into the hardware.”\textsuperscript{92} To change the IMEI, you have to buy a new device.\textsuperscript{93}

Advertising Identifiers (Ad IDs) also “uniquely identify mobile devices.”\textsuperscript{94} Ad IDs are incorporated into iOS and Android systems.\textsuperscript{95} These Ad IDs are similar to cookies on the internet, except they are shared with apps.\textsuperscript{96} Ad IDs exist for one reason, “[t]o link user activity across apps on a device.”\textsuperscript{97} Users can change Ad IDs, reset them, and on some devices turn the Ad IDs off.\textsuperscript{98} But Ad IDs “are enabled by default on both iOS and Android, and are available to all apps without any special permissions.”\textsuperscript{99} With this default setting, most individuals do not realize they can turn them off or what these Ad IDs are doing in the background.\textsuperscript{100}
Browser fingerprinting is another method to unmask individuals. Browser fingerprinting exists “to circumvent the normal controls users have that enable them to control their own browsers.” Browser fingerprints are “[t]he various properties of your web browser and computer that a website can notice when you visit.” Each aspect of your computer—such as the operating system, graphics card, and browser version—helps form a fingerprint. The more aspects collected, the more unique of a fingerprint that can be created.

An example is helpful to understand how browser fingerprints differ from identifiers that can be blocked or changed. Imagine a GPS tracker attached to you. As you walk around, that GPS locator will ping your location. However, as soon as you discover the GPS tracker and discard it, the GPS tracker is useless. For cookies, IP addresses, and other identifiers that can be blocked or changed the same holds true. In contrast, browser fingerprinting is “more permanent”. This type of unmasking is equivalent to “tracking a car by its license plate, make, model, and color.” These traits are difficult—if not impossible—to change.

There are other identifiers that, although not linked to your phone or computer, are just as useful to unmask someone. Automatic License Plate Readers (ALPR) are cameras that “can automatically identify and record license plate numbers on passing cars.” It is illegal to cover your license plate, and every car must have one to comply with state law. Private companies use ALPRs to gather location data on where you travel and then sell this data. Companies also collect biometrics, such as fingerprints and facial recognition. Biometrics can provide insight into behavior, help verify individuals, and provide

---

101 Id. at 15, 17.
103 Browser Fingerprint, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/glossary/browser-fingerprint [https://perma.cc/A6NW-HSQT].
104 CYPHERS & GEBHART, supra note 12, at 16.
105 Id. at 15, 17.
106 Cover Your Tracks, ELEC. FRONTIER FOUND., https://coveryourtracks.eff.org/learn [https://perma.cc/AN5M-M9V5].
107 Id.
108 Id.
109 Id.
110 Id.
111 Id.
112 CYPHERS & GEBHART, supra note 12, at 21.
113 Id.
114 Id.; SHENKMAN ET AL., supra note 34, at 34.
access to buildings, devices, and banking systems.\textsuperscript{115}

III. DATA BROKERS AND NATIONAL SECURITY

Data brokers can provide governments with high-value intelligence.\textsuperscript{116} Think of phone location data. Where someone’s phone is at night on a consistent basis likely shows their home; where someone’s phone is during the day on a consistent basis likely indicates their office.\textsuperscript{117} Once a government has this information, it could start to target individuals who work at places of interest, such as a company that creates highly classified weapon systems. And by combining data sets, governments could find the right personnel with the right weaknesses to gain access to these weapon systems. Data broker information also provides governments a pathway to extort individuals, impersonate them, influence how they think, or use the information to surveil them.\textsuperscript{118}

Data brokers can also provide information on equipment and facilities. For equipment, data brokers can deliver what signals the device emits, the ID for the device, and specifications for the device.\textsuperscript{119} This information can expose what type of device exists, can help map where the device is located, and could even help someone hack the device.\textsuperscript{120} For facilities, data brokers can offer geolocation data on sensitive facilities and who is going in and out of those facilities.\textsuperscript{121}

Data brokers offer all this information—and more—as a cheaper alternative to traditional intelligence.\textsuperscript{122} Human assets, satellites, and expensive operations are generally necessary for one form or another of

\textsuperscript{115} Shenkman et al., supra note 34, at 34.
\textsuperscript{116} Henrik Twetman & Gundars Bergmanis-Korāts, Data Brokers and Security 9 (2021).
\textsuperscript{119} Twetman & Bergmanis-Korāts, supra note 116.
\textsuperscript{120} Id.
\textsuperscript{121} Id.
intelligence. Human assets require training, such as covert operation and language training. Satellites require high-tech software and materials. These are just a few examples of “highly resource-intensive and cost-prohibitive” requirements in normal intelligence. In contrast, purchasing data on targets from data brokers is much simpler and more efficient. The increasing reliance on technology provides data brokers the opportunity to scale their product as well. As this occurs, data brokers will increase in size, capability, and impact.

A couple years ago, The New York Times demonstrated how valuable data brokers can be. It used data broker information to identify “individuals belonging to the President’s Secret Service detail.” By obtaining a “dataset with more than 50 billion location pings from the phones of more than 12 million people in this country,” The New York Times unmasked the location data and tracked President Trump’s location. This process only took a few minutes.

A. National Security Perils

Data can create chaos for the United States. Back in 2013, U.S.
intelligence realized that its operatives “were being rapidly and successfully identified by Chinese intelligence.” The Central Intelligence Agency (CIA) did not understand how the Chinese were accomplishing these feats with such accuracy and speed. Some thought there could be a mole or perhaps secret communications had been intercepted. In the end though, the likely answer was data—stolen by the Chinese. U.S. officials believed that China had combed through this data, synthesized it, and then re-purposed it for intelligence operations. Along the same lines, Russian intelligence exploited discrepancies in payroll data at the U.S. Embassy in Moscow, allowing them to identify CIA personnel working at the Embassy.

Foreign adversaries can collect this data through hacking. In 2015, the Chinese hacked the Office of Personnel Management (OPM), resulting in one of the most catastrophic data breaches in U.S. history. In total, the Chinese gathered intelligence on “21.5 million current and former U.S. officials, their spouses, and job applicants, including health, residency, employment, fingerprint, and financial data.” As part of this haul, the Chinese gained insight into U.S. officials’ security clearance investigations. These investigations revealed people’s most closely kept secrets, including their mental health, sexual histories, and whether their relatives could be subject to blackmail. In recent years, China has hacked major health insurance providers, hotel chains, and major airlines too—resulting in a coup to obtain more sensitive data on U.S. citizens.

Data does not exist in a vacuum though—especially for our adversaries. When combined with other data, such as travel itineraries,

---

133 Dorfman, supra note 118.
134 Id.
135 Id.
136 Id.
137 Id.
138 Id.
139 Tvetman & Bergmanis-Korats, supra note 116, at 22.
141 Id.
142 Dorfman, supra note 118.
143 Id.
information from the OPM breach “likely provided Chinese intelligence potent clues about unusual behavior patterns, biographical information, or career milestones that marked individuals as likely U.S. spies.” In the future, by combining information from the OPM hack and data broker information, China “could [continue to] identify a good number intelligence operatives that go to mainland China every year.” Or it could help China in a conflict over Taiwan for targeting and intelligence operations. China could also use this information to help others create chaos. For example, it could analyze and synthesize this information and provide the results to Iran or Russia. Once this information is provided to foreign adversaries like Iran, it could turn and sell that info to proxy terrorist groups. The options are endless.

B. National Security Benefits

Compared to its foreign adversaries, the U.S. Government is at a disadvantage when it comes to data. There are numerous reasons why. Some countries constantly collect data on their citizens, increasing their data pool (e.g., China). Other countries do not have developed economies; therefore, their citizens do not produce as much data as a developed country, such as the U.S. Another reason is that data collection laws in some countries are stricter than in the U.S., limiting the amount of data produced and collected (e.g., Europe). As such, the United States outproduces most countries in collectable data, providing a ripe target for its foreign adversaries. A natural byproduct of this landscape is foreign adversaries collecting a greater amount of data than the U.S.

Nevertheless, the U.S. understands the value of data. A few

145 Dorfman, supra note 118.
146 Telephone Interview with Gail Helt, Former CIA Analyst, East Asia and Southeast Asia (Mar. 22, 2023).
147 Id.
148 Id.
149 Id.
150 Id.
151 Telephone Interview with Duyane Norman, supra note 17.
152 Id.
153 Id.
154 Id.
155 Id.
156 Id.
157 Bennett Cyphers, How the Federal Government Buys Our Cell Phone Location Data, ELEC. FRONTIER FOUND. (June 13, 2022),
years ago, the U.S. Army funded a project that used data broker data “to track movements around Russian missile test sites, including those of high-level diplomats.”158 The Iowa National Guard also joined the shift to data brokers: they purchased a 1-year data broker license.159 In 2020, Special Operations Command (SOCOM) purchased over half a million dollars of services from a data broker.160 As part of its sales pitch, this data broker showed SOCOM the data’s value: using the data, the data broker “tracked phones of Russian soldiers amassed on the Ukrainian border to show where they had come from, and it tracked 183 devices that had visited both the NSA and CIA headquarters to show where American intelligence personnel might be deployed.”161 SOCOM confirmed that data broker purchases were to “support Special Operations Forces mission requirements overseas.”162

U.S. federal agencies have joined the data broker fray as well. The Department of Homeland Security (DHS) and two divisions under DHS, Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE), have purchased “commercially available cell phone location records.”163 DHS has purchased “at least $2 million of location data” from data brokers.164 Since 2018, ICE has purchased utility data, location data, and license plate reader data from data brokers, using this data for immigration enforcement.165 In one instance, ICE used data “to


159 Cyphers, supra note 157.

160 Id.

161 Id.

162 Id.


164 Cyphers, supra note 157.

165 Id.; Tau, supra note 158; SHENKMAN ET AL., supra note 34, at 31.
detect cellphones moving through what was later discovered to be a
tunnel created by drug smugglers between the U.S. and Mexico that
terminated in a closed Kentucky Fried Chicken outlet on the U.S. side
near San Luis, Arizona. CBP has used data broker information to
search for unusual cellphone activity, “including unpopulated
portions of the US-Mexico border.” This data also helped CBP locate
tunnels along the border. The Federal Bureau of Investigation (FBI), Drug
Enforcement Agency (DEA), Internal Revenue Service (IRS), Defense
Intelligence Agency (DIA), and Secret Service have purchased
information from data brokers as well.

IV. ASSESSMENT OF THE REGULATORY LANDSCAPE

Some believe U.S. Government purchases of data from data
brokers violates the Fourth Amendment. Some scholars do not. Their
arguments for and against their position rests on a recent Supreme
Court case, Carpenter v. United States. In Carpenter, the Supreme
Court explained that the Fourth Amendment mandates that the U.S.
Government obtain a warrant to search a person’s cell-site location
information from a company. The DIA’s position is that Carpenter,
and in turn the Fourth Amendment, does not “require a judicial warrant
to purchase or use commercially-available data for intelligence

166 Tau, supra note 158.
167 Cyphers, supra note 157.
168 Id.
170 See Dori H. Rahbar, Laundering Data: How the Government’s Purchase of Commercial Location Data Violates Carpenter and Evades the Fourth Amendment, 122 COLUM. L. REV. 713 (2022); Canaan, supra note 163, at 97–98.
171 Orin Kerr, Buying Data and the Fourth Amendment, 2109 HOOVER WORKING GRP. ON NAT’L SEC., TECH., & LAW, AEGIS SERIES PAPER 1 (2021).
purposes.”174 If the Fourth Amendment does apply here, the only real legal remedy for a violation is suppression and exclusion in a criminal case.175 But this paper need not analyze whether Carpenter does or does not apply here because at least one U.S. federal agency (likely several more) believes it does not.176 Thus, these agencies will continue to follow that interpretation until the courts or Congress weigh in.

Although there are numerous statutes that appear to limit the U.S. Government’s purchasing power with data brokers—they do not.177 One statute in particular is worth discussing, the Privacy Act of 1974.178 At bottom, this statute “limits the government’s use and sharing of records between federal agencies.”179 So the statute limits actions between different agencies but does not apply to private companies.180 Therefore, data brokers can sell as much data as they would like to individual government agencies.181

Executive Order (E.O.) 12333 governs intelligence agencies’ purchases from data brokers.182 This E.O. explains that “publicly available information” can be collected on U.S. persons.183 “Each of the 17 components of the Intelligence Community issues its own guidelines” on its interpretation of E.O. 12333.184 For at least some agencies, including the DoD and CIA, publicly available information includes “commercially available data”, i.e., data from data brokers.185

At bottom, current laws and regulations allow data brokers to sell consumer data to the U.S. Government and foreign adversaries.186

A. Self-Regulation

“Companies have shared responsibility for protection of

174 U.S. DEF. INTEL. AGENCY, CLARIFICATION OF INFORMATION BRIEFED DURING DIA’S 1 DECEMBER BRIEFING ON CTD (2021) (emphasis added).
175 Rahbar, supra note 170, at 713; Canaan, supra note 163, at 97–98.
176 See U.S. DEF. INTEL. AGENCY, supra note 174.
177 Canaan, supra note 163, at 107.
180 Id.
181 Id.
182 SHENKMAN ET AL., supra note 34, at 19.
183 Id.
184 Id.
185 Id. at 20.
186 Wyden, supra note 1.
America.”¹⁸⁷ Think back to World War II when the “arsenal of democracy” mobilized to defeat tyranny spreading across the globe. From small businesses to the largest corporations, there was a single goal: win the war. Does this mindset still exist today? To be sure, the U.S. is not in a state of war—especially not a world war—and companies do operate in a much different global economy now. However, U.S. companies exist because the “western world has a value system” that allows them to do so; values like a belief in free-markets, freedom of speech, and many others.¹⁸⁸ As such, companies must act with a conscience and police products they create to protect U.S. national security—they have a moral obligation to do so.¹⁸⁹

With this in mind, companies that run app stores “are in a unique position to protect tech users from app-powered surveillance.”¹⁹⁰ The companies behind the app stores are sovereign—they can make decisions unilaterally. Unlike government legislation or regulation, which are generally slow and bureaucratic, companies can institute change overnight. Google and Apple have instituted bans against some data brokers.¹⁹¹ In similar fashion, companies with control over app stores could require that data not be shared or sold to foreign adversaries.¹⁹² Those who support self-regulation explain that “comprehensive [government] legislation is too inflexible and time-dependent to keep up with the fast-moving world of information technology.”¹⁹³ In contrast, companies can move at the speed of innovation.

Companies only have so much power though. Companies could require disclosure from data brokers on who they sell data to, but that policy would “rely heavily on the honor system.”¹⁹⁴ And discovery of violations is not always easy.¹⁹⁵ Even if a violator was discovered, companies could only rid their app stores of a data broker for violating

¹⁸⁷ Telephone Interview with Duyane Norman, supra note 17.
¹⁸⁸ Id.
¹⁸⁹ Id.
¹⁹¹ Id.
¹⁹² Canaan, supra note 163, at 114–16.
¹⁹³ Kuempel, supra note 15, at 216.
¹⁹⁵ Id.
their policy—no further discipline could be taken against violators.\textsuperscript{196} Another issue is that not all companies will take a strong stance against data brokers—leaving a fragmented approach.\textsuperscript{197} Self-regulation remains voluntary and unenforceable.\textsuperscript{198} This reality is not to say that self-regulation does not have a place in this endeavor, but alone it is insufficient.\textsuperscript{199}

There has been an interesting development in the self-regulation world recently. Capitalism abhors a vacuum—and that applies to the issues surrounding the data broker world. As a result, companies, such as Known Privacy, have created products for companies to ban data brokers from collecting its employees’ data.\textsuperscript{200} Known Privacy and its ilk are pitching their product as beneficial in two ways: 1) it protects employees from scams, identity theft, and phishing attempts; and 2) it protects companies from bad actors gaining access to their systems and files.\textsuperscript{201} Although these companies cannot solve the data broker issue alone, it is important that American ingenuity is attempting to address the issue. There is one concern underlying this ingenuity though: foreign adversaries can prop up these opt-out services, cloaking their true intentions with “good deeds.”

B. Consent by User

Often times, companies view consent as “a person simply using an application or service that has a privacy policy.”\textsuperscript{202} This is not consent.\textsuperscript{203} Consumers do not fully understand or know how their data is “collected, used, and possibly sold or shared” from simple usage.\textsuperscript{204} Some companies do not even require reading a privacy policy. For example, TikTok says that by using its service, you agree to its privacy policy.\textsuperscript{205} And even if consumers did understand a privacy policy, they would likely not understand the harm their data can cause.\textsuperscript{206}

As a result, most consumers do not have the ability to

\textsuperscript{196} Id.
\textsuperscript{197} Kuempel, supra note 15, at 217–18.
\textsuperscript{198} Palk & Muralidhar, supra note 14, at 784–85; Kuempel, supra note 15, at 217–18.
\textsuperscript{199} Canaan, supra note 163, at 114–16.
\textsuperscript{201} Id.
\textsuperscript{202} Sherman et al., supra note 22, at 3.
\textsuperscript{203} Id.
\textsuperscript{204} Id.
\textsuperscript{205} Id. at 19.
\textsuperscript{206} Id. at 20; Palk & Muralidhar, supra note 14, at 784–85.
meaningfully control their data. To truly opt out of data broker tracking “is like opting out of electricity, or cooked foods—you are free to do it in theory”; in practice, it means “opting out of much of modern life.” Consumers can help try to limit their data, but this approach will have little to no effect on the amount of data collected by data brokers—and then sold around the globe.

C. FTC Regulation

Some argue that the “FTC is the most suitable agency to be utilized for enforcement of data protection.” The FTC is the only federal agency empowered to protect consumers and regulate competition issues in the economy. Because it is an agency with a focus on consumers, the FTC can adapt quicker and provide more expertise than Congress. In addition, any rules proposed by the FTC would “require thorough input”. With this input, the FTC could help ensure that proper regulations are tailored for the issues at hand. Lastly, Congress could tailor the FTC’s authority in this arena to ensure that the FTC focus on the issues that Congress wants it to focus on.

As part of its mission, the FTC prevents “unfair acts or practices in two ways: formal rulemaking and case-by-case litigation.” For formal rulemaking, the FTC can establish rules “which define with specificity” unfair acts or practices under Section 5(a). “Once a rule takes effect, it becomes in essence an addendum to Section 5(a)'s phrase ‘unfair . . . acts or practices’”. These rules can then be enforced in

207 Palk & Muralidhar, supra note 14, at 784–85.
208 CHRISTL, supra note 11, at 5.
209 Sherman et al., supra note 22, at 18.
213 Id.
214 Id.
215 Id.
218 LabMD, 894 F.3d at 1231.
federal district court.\(^{219}\)

The other option is establishing an “unfair act or practice through litigation.”\(^{220}\) If litigation results in an act or practice being “adjudged to be unfair, the act or practice becomes in effect—like an FTC-promulgated rule—an addendum to Section 5(a).”\(^{221}\) For litigation, the FTC can “prosecute its claim” in front of an Administrative Law Judge (ALJ) or federal district judge.\(^{222}\) Appellate review for the former approach occurs before the FTC commission then in a federal court of appeals; appellate review for the latter approach occurs in a federal court of appeals.\(^{223}\) If the ALJ rules in favor of the FTC, the ALJ will issue a cease and desist order; “the district court issues an injunction”.\(^{224}\) Both have the same effect and command: “discontinue engaging in a specific unfair act or practice.”\(^{225}\)

In a recent lawsuit against a data broker, the FTC alleged that the data broker’s “sale, transfer, or licensing of precise geolocation data associated with unique persistent identifiers that reveal consumers’ visits to sensitive locations is an unfair practice, in violation of the FTC Act.”\(^{226}\) The FTC’s lawsuit signals a shift in their approach: it is the first time they have “claimed that it is per se unfair to sell such data if it reveals sensitive locations.”\(^{227}\) However, winning this case will prove difficult. This case will likely hinge on injury—whether this data broker’s actions will “cause or are likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves, and is not outweighed by countervailing benefits to consumers or competition.”\(^{228}\) In its complaint, the FTC did not allege any actual examples of data-induced

\(^{220}\) LabMD, 894 F.3d at 1231.
\(^{221}\) Id.
\(^{222}\) Id.
\(^{223}\) Id.
\(^{224}\) Id. at 1233–34.
\(^{225}\) Id. at 1233.
\(^{228}\) Id.
Injury. Instead, the FTC explained that the data broker’s disputed practices could be used to cause harm. This case is still ongoing but whatever the outcome, the results will either reign in the FTC’s reach or put data brokers in the FTC’s crosshairs.

D. Legislative

Some policymakers have an appetite to regulate data brokers. Over the last couple years, different congressional members have introduced bills related to data brokers. If signed into law, The Fourth Amendment is Not for Sale Act would prohibit data brokers from selling U.S. citizen data to law enforcement and intelligence agencies “without court oversight”. The Protecting Americans’ Data From Foreign Surveillance Act “would create export controls for sensitive U.S. user data”, such as health information and information on military members. It would also force the Secretary of Commerce “to identify which types of personal data could harm U.S. national security and designate which countries would require licenses to export to or be denied as a default.” The Protecting Military Service Members’ Data Act of 2022 would prevent “data brokers from selling lists of military personnel to adversarial nations including China, Russia, Iran, and North Korea.” All three bills have bipartisan support; all three bills have also stalled in Congress.

There is also state legislation trying to address data broker issues. Two examples are Vermont and California. Vermont now

---

229 Id.
230 Id.
231 Kans, supra note 9.
233 Szymanski, supra note 8; Kans, supra note 9; Wyden, supra note 232.
235 Id.
237 Ng, supra note 179.
requires “companies that buy and sell third-party data to register with the secretary of state”. California passed a law that allows consumers to “access the personal information that brokers have about them for free, and to opt out of having their data sold”. At bottom, both laws are about disclosure, not restrictions on data brokers’ abilities to buy, sell, and share data. Moreover, these laws distinguish between data that is personally identifiable and data that is not. However, as this paper has explained, those lines are increasingly blurred.

V. Privacy Issues for U.S. Citizens

One must acknowledge that America was founded on a distrust of government. This tradition continues into the 21st century—and may be even stronger because of the tools at the U.S. Government’s fingertips.

Data brokers are one of those tools. Their business model creates an “open book” of a person’s life—omniscience for sale. If the U.S. government had collected this data through its own intelligence methods, U.S. citizens would be in an uproar. So why should there be a different reaction to purchasing this information from data brokers?

One need not be a conspiracy theorist to have hesitation about the U.S. Government having access to this type of information. Nor does one need to be creative to think how bad actors within the U.S. Government could abuse this type of information. With data from data brokers, “the [U.S.] government could pursue personal vendettas, target the politically unpopular, and trample on other civil liberties.”

Personal data from data brokers includes “precise geolocation, internet history, [political preferences], communications, audio and visual

---

238 Canaan, supra note 163, at 118–20; VT. STAT. ANN. tit. 9, § 2431 (2012).
239 Canaan, supra note 163, at 120.
240 Statement of Justin Sherman, supra note 140.
241 Id.
242 Id.
244 Id.
245 Arango, supra note 173, at 739 (“In 1963, the Federal Bureau of Investigation wiretapped the phones of Martin Luther King, Jr. under the pretense of determining King’s ties to members of the American Communist Party. And after 9/11, the New York Police Department, with significant assistance from the Central Intelligence Agency, spent years monitoring Muslim neighborhoods and community centers.”).
footage, and biometrics.”

If the U.S. Government chose to do so, this type of information could be used for a litany of actions: investigations, prosecutions, or simply to harass citizens. Although there are numerous examples of the U.S. Government flaunting civil liberties, there may be none more famous than the FBI attempting to discredit and destroy Martin Luther King, Jr. An oft-forgotten example occurred several years before the MLK smear campaign: the internment of Japanese Americans during World War II. Imperfect governments produce imperfect results—and no government is perfect.

Even if the U.S. Government does not improperly use this data, it is vulnerable to hacks and breaches. As explained, these types of breaches have become more and more frequent. To be sure, private companies are vulnerable to these types of attacks as well. However, the U.S. Government’s track record suggests that private companies infrastructure and cybersecurity is better suited to protect data. Moreover, the U.S. Government is gobbling up data from all types of different data brokers, creating a target ripe for exploitation—not just for foreign adversaries either. Scammers have used data to swindle families, veterans, and other American citizens. Data broker information has also been used “to hunt down and stalk, intimidate, harass, and even murder individuals.”

*The New York Times* demonstrated how easy data could be used to violate one’s civil liberties. With just location data, a couple journalists were able to track service members as they drove home and law enforcement as they dropped their kids off at school. When other data points from data brokers are combined, privacy concerns increase exponentially.

Even if not misused, this data’s existence can have harmful

---

247 SHERMAN, supra note 42, at 3, 9.
248 Id.
250 SHERMAN, supra note 42, at 3.
251 Id.
252 See Thompson & Warzel, supra note 243.
253 Id.
254 Id.
effects.255 “If people know they’ll be tracked, it will certainly make them think twice before linking themselves to a movement.”256 And the fact that the U.S. Government has this info could cause enough concern that people start to act differently. For example, in China, “omnipresent tracking has fundamentally changed the democratic protests in Hong Kong.”257 Although non-authoritarian countries may not use surveillance in the same manner, its existence can have a similar effect.

VI. WAY FORWARD

There are two issues that must be addressed here. The first is data broker sales to foreign adversaries. The other is data broker sales to the U.S. Government.

A. Foreign Adversaries

Legislation will not prevent intelligence issues created by data brokers.258 As long as data exists, foreign adversaries can and will exploit it.259 And they have many options at their disposal to do so: hacking the U.S. Government; hacking data brokers; purchasing from data brokers; setting up third-party companies to purchase from data brokers; or hacking the source of the data (e.g., Hilton Hotels). In other words, if not through purchasing power, foreign adversaries can gather data through espionage or theft.260 To truly keep data out of foreign adversaries’ grasp, the U.S. Government would have to “limit its existence in the first place”—an unworkable solution.261 In fact, “[i]ntelligence officers don’t trust that legislation is preventing the data that exists is not ending up in adversary hand—[they] assume [the] worst, plan for the worst.”262 For the U.S. Government, the intelligence

256 Id.
257 Id.
258 Telephone Interview with Duyane Norman, supra note 17.
259 Id.; Telephone Interview with Gail Helt, supra note 146; Telephone Interview with Annie Fixler, Ctr. Cyber Tech. Innovation Dir. & Rsch Fellow at Found. for Def. of Democracies (Mar. 31, 2023).
260 Interview with Kirsten Hazelrig, supra note 126; Telephone Interview with Duyane Norman, supra note 17; Telephone Interview with Gail Helt, supra note 146.
261 Interview with Kirsten Hazelrig, supra note 126.
262 Telephone Interview with Duyane Norman, supra note 17.
focus must be on how to adapt in this new environment.\textsuperscript{263}

Even so, legislation can provide U.S. law enforcement the ability to hold companies accountable for assisting foreign adversaries.\textsuperscript{264} Although this legislation will not prevent foreign adversary collection of this data—it will likely slow it. Moreover, from a legal and moral perspective, the U.S. Government should not allow companies to assist foreign adversaries.

This legislation requires several tenets. First, data brokers must be properly defined: a data broker is any company that brokers data, i.e., sells, trades, or shares data. Otherwise, many companies that engage in data-broker-like sales and contracts will not be limited from providing data to foreign adversaries.\textsuperscript{265} Second, to provide a stronger enforcement mechanism, similar to 18 U.S.C. § 2339B (Material Support to Terrorism statute), data broker legislation should allow the U.S. Government to prosecute companies that knowingly sell data to foreign adversaries, including through front companies. For behavior that does not rise to the “knowingly” level, civil penalties will suffice. Third, a private right of action is crucial for this legislation.\textsuperscript{266} Why? “While government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate.”\textsuperscript{267} Individual citizens and groups of individuals (class actions) will be a powerful tool to keep companies accountable.\textsuperscript{268} Adding a private right of action would also be in line with legal norms surrounding other privacy laws.\textsuperscript{269}

The legislation discussed in this paper should also be considered as blueprints for any legislation. To be sure, no legislation presented is a perfect solution. For example, \textit{The Protecting Military Service Members’ Data Act of 2022} focuses only on service members data being

\begin{flushright}
\textsuperscript{263} Id.
\textsuperscript{264} Id.
\textsuperscript{265} Statement of Justin Sherman, \textit{supra} note 140.
\textsuperscript{266} Statement of Caitriona Fitzgerald, \textit{supra} note 16.
\textsuperscript{267} Id.
\textsuperscript{268} Id.
\textsuperscript{269} Id. (“For example, when Congress passed the Cable Communications Privacy Act in 1984, they established privacy rights for cable subscribers and created a private right of action for recovery of actual damages not less than liquidated damages of $100 per for violation or $1,000, whichever is higher. The Video Privacy Protection Act specifies liquidated damages of $2,500.61. The Fair Credit Reporting Act affords individuals a private right of action that can be pursued in federal or state court against credit reporting agencies, users of credit reports, and furnishers.”).
sold to foreign adversaries. As this paper explains, service members are not the only ones that need to be protected—all Americans do. There are plenty of civilians that foreign adversaries would want information on. But the legislation mentioned earlier in this paper provides a solid starting point for anyone attempting to regulate the data broker industry and protect U.S. national security.

B. U.S. Government

The U.S. Government should not be able to purchase U.S. citizen data from data brokers. Data brokers collect billions of data points on U.S. citizens—without their express consent or knowledge. A government that can pull these resources together creates a surveillance apparatus once thought impossible. One must not lose sight of what these data points offer insight into: “ethnicity, religious and political views, relationship status, sexual orientation, and alcohol, cigarette, or drug use as well as personality traits such as emotional stability, life satisfaction, impulsivity, [and] depression.” The data is not just 1s and 0s—the data is our lives—blemishes and all. Most would not want neighbors to have this information, let alone a government. Indeed, the U.S. Government can use this information for good, but just like the Janus coin, the inverse is also true: the data can be used for harm.

To be clear, limiting the U.S. Government access to data broker information on U.S. citizens is not a wholesale ban on data brokers. Data brokers collect billions of data points, including on foreign nationals. The U.S. Government is free to purchase foreign national data from data brokers, which will allow it to still improve machine learning and intelligence operations.

Before enacting data broker legislation, Congress should investigate whether better funding and resources to agencies charged with carrying out these laws is necessary. Although some believe the

271 Sherman, et al., supra note 22, at 10; Kans, supra note 9; Palk & Muralidhar, supra note 14 at 820–21; Fed. TRADE COMM’N, supra note 24, at IV.
272 CHRISTL, supra note 11, at 71.
273 Interview with Johnathan Rudy, supra note 51.
274 Telephone Interview with Gail Helt, supra note 146.
FTC is the best agency to control data brokers, that may not be the case. Its current lawsuit will shed light of its application on Section 5(a); however, it does seem to be a misapplication. This new legislation seems better suited for the Department of Commerce or Treasury to enforce and any criminal actions would be handled by the Department of Justice. However, this paper need not pinpoint the exact role for agencies here. What is important to note is that agencies must be empowered and properly resourced to enforce these new laws. Otherwise, the laws serve no purpose.

Private companies need to shoulder some burden here too. U.S. national security is a concern to anyone that lives in the U.S. Companies that create data, collect data, or both have to realize how powerful that data is. Once properly understood, companies should look at how they are fueling the “modern surveillance economy”, seeking ways to limit their support. Companies like Known Privacy should also continue to create and offer programs that limit data collection.

The preferred solution is that the U.S. Government should not be allowed to purchase U.S. citizen data from data brokers. However, if policy makers disregard this recommendation and continue to allow the U.S. Government to do so, then new rules need to govern these purchases. First, when the U.S. Government purchases data about Americans, it must inform Congress about the purchase, what type of data was purchased, and how the data will be used. Second, Congress must dictate cybersecurity enhancements prior to acquisition from data brokers by any government entity. In keeping with this security mindset, U.S. Government agencies that hold this information should also undergo “regular independent audits to assess the agency’s use of such data.”

Some argue that the U.S. Government’s guardrails ensure that data is not used improperly. But this argument does not survive closer examination. One glaring example on why the U.S. Government should not collect this data: Edward Snowden. When Snowden was at the National Security Agency, there were guardrails in place too. Yet he was still able to steal and leak 1.7 million highly sensitive documents. Insider threats exist; there is no method for the U.S. Government to completely protect itself from these threats nor should anyone expect it

---

275 SHENKMAN ET AL., supra note 34, at 38.
276 Id. at 40.
too.\textsuperscript{278} Once the U.S. Government gobbles up data from data brokers, it provides a one-stop-shop for packaged data, inferences and all. In fact, an insider threat is not even necessary: China and other adversaries have demonstrated that the U.S. Government’s cybersecurity is hackable.

Another argument others offer in support of the U.S. Government here is that data from data brokers is anonymized. But as experts have shown, anonymization becomes less possible every day. The combination of infinite data with 21st century computing power allows companies and governments alike to unmask data sets. Data may arrive “anonymous”, but it need not remain that way.

VII. CONCLUSION

For foreign adversaries, the data Pandora’s box has been opened—there is no closing it. Yet, the U.S. must still police those who operate within its borders. Even though these actions will potentially only slow the inevitable, there is a moral and ethical obligation to prevent U.S. companies from helping foreign adversaries. There is also a moral and ethical obligation to protect U.S. citizens’ data from foreign adversaries. Once enacted, this approach will have global implications as well, helping establish international norms.

One must acknowledge the benefits that data brokers offer the U.S. Government. This data is cheap and accessible; it’s neatly packaged and can be sorted through filters; and it can provide insight into intelligence the U.S. Government desires: information on weapon systems, where people work, pressure points to use against them, and locations of facilities. \textit{The New York Times} demonstrated this power, leading to the question: What more could a first-world country do?

But the U.S. should not compromise its values to keep pace with its foreign adversaries. If it does, herein lies a dangerous path. Its adversaries will always flaunt human rights and U.S. norms. Similar to war, autocracies and dictatorships have the initial advantage in this data war. But, also similar to war, democratic values need not be compromised to overcome this initial advantage. The U.S. has found ways to defeat foreign adversaries in the past without doing so—and can do so in the future.
