JUNE 2023

# Surveillance for Sale

## *The Underregulated Relationship between U.S. Data Brokers and Domestic and Foreign Government Agencies*

AUTHOR
Caitlin Chin

A Report of the CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JUNE 2023

# Surveillance for Sale

## *The Underregulated Relationship between U.S. Data Brokers and Domestic and Foreign Government Agencies*

AUTHOR
Caitlin Chin

A Report of the CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

# About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).



## Acknowledgments

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report. The author would like to thank the experts who participated in discussions and interviews during this project under the Chatham House rule. In addition, the author would like to thank the CSIS publications and iLab team for their copyediting, review, and design of this report.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

# Contents

# Introduction

Ten years ago, when whistleblower Edward Snowden revealed that U.S. government agencies had intercepted bulk telephone and internet communications from numerous individuals around the world, President Barack Obama acknowledged a long-standing yet unsettled dilemma: "You can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. . . . There are trade-offs involved."[1]

Snowden's disclosures reignited robust debates over the appropriate balance between an individual's right to privacy and the state's interest in protecting economic and national security—in particular, where to place limitations on the U.S. government's ability to compel access to signals intelligence held by private companies.[2] These debates continue today, but the internet landscape—and subsequently, the relationship between the U.S. government and private sector—has evolved substantially since 2013. U.S. government agencies still routinely mandate private companies like Verizon and Google hand over customers' personal information and issue nondisclosure orders to prevent these companies from informing individuals about such access.[3] But the volume and technical complexity of the data ecosystem have exploded over the past decade, spurred by the rising ubiquity of algorithmic profiling in the U.S. private sector. As a result, U.S. government agencies have increasingly turned to "voluntary" mechanisms to access data from private companies, such as purchasing smartphone geolocation history from third-party data brokers and deriving insights from publicly available social media posts, without the formal use of a warrant, subpoena, or court order.

In June 2023, the Office of the Director of National Intelligence (ODNI) declassified a report from January 2022—one of the first public efforts to examine the "large amount" of commercially available information that federal national security agencies purchase.[4] In this report, ODNI recognizes that sensitive personal information both "clearly provides intelligence value" but also increases the risk of harmful outcomes like blackmail or harassment. Despite the potential for abuse, the declassified report reveals that some intelligence community

elements have not established proper privacy and civil liberties guardrails for commercially acquired information and that even ODNI lacks awareness of the full scope of data brokerage contracts across its 18 units. Critically, the report recognizes that modern advancements in data collection have outpaced existing legal safeguards: "Today's CAI [commercially available information] is more revealing, available on more people (in bulk), less possible to avoid, and less well understood than traditional PAI [publicly available information]."

The ODNI report demonstrates how the traditional view of the privacy-security trade-off is becoming increasingly nuanced, especially as gaps in outdated federal law around data collection and transfers expand the number of actors and risk vectors involved. National Security Adviser Jake Sullivan recently noted that there are also geopolitical implications to consider: "Our strategic competitors see big data as a strategic asset."[5] When Congress banned the popular mobile app TikTok on government devices in the 2023 National Defense Authorization Act (NDAA), it cited fears that the Chinese Communist Party (CCP) could use the video-hosting app to spy on Americans.[6] However, the NDAA did not address how numerous other smartphone apps, beyond TikTok, share personal information with data brokers—which, in turn, could transfer it to adversarial entities. In 2013, over 250,000 website privacy policies acknowledged sharing data with other companies; since then, this number inevitably has increased.[7] In a digitized society, unchecked data collection has become a vulnerability for U.S. national security—not merely, as some once viewed, a strength.

The reinvigorated focus on TikTok's data collection practices creates a certain paradox. While politicians have expressed concerns about Chinese government surveillance through mobile apps, U.S. government agencies have purchased access to smartphone geolocation data and social media images related to millions of Americans from data brokers without a warrant. The U.S. government has simultaneously treated TikTok as a national security risk and a handy source of information, reportedly issuing the app over 1,500 legal requests for data in 2021 alone.[8] It is also important to note that national security is not the only value that can come into tension with information privacy, as unfettered data collection carries broader implications for civil rights, algorithmic fairness, free expression, and international commerce, affecting individuals both within and outside the United States.

*The ODNI report demonstrates how the traditional view of the privacy-security trade-off is becoming increasingly nuanced, especially as gaps in federal law around data collection and transfers expand the number of actors and risk vectors involved.*

Technological advancements warrant a reexamination of the traditional privacy-security trade-off—one that prioritizes forward-looking guardrails around emerging trends in data analytics, particularly the rising ubiquity of commercially available information. This report attempts to bridge these gaps by analyzing the relationship between the U.S. data brokerage industry and domestic and foreign government agencies. It first explains how private companies have built up massive troves of personal information, which data brokers aggregate and sell to both public and private sector entities without proper safeguards to protect privacy and civil liberties.[9] Then it analyzes U.S. privacy developments alongside those in the European Union, Canada, and China, illustrating

how even governments that have recently modernized their data protection frameworks still have not fully addressed voluntary access to private sector data. [10] Ultimately, it illustrates how stricter U.S. data privacy regulations in the private and public sectors will strengthen the national security, human rights, and economic interests of the United States rather than hobble its geopolitical competitive position.

# Background

## *How Data Brokers Operate*

Over the past decade, popular consumer-facing devices, websites, and apps have built up increasingly sophisticated surveillance capabilities due to several trends. For one, data storage has become more affordable, creating incentives for companies to retain data even when it is no longer needed for the purpose for which it was originally collected. In addition, widespread deployment of predictive algorithms across all sectors has generated high demand for personal information.[11] As a result, numerous digital platforms now operate their business models around sharing detailed user information with advertisers, private corporations, individuals, or government agencies—often through third-party intermediaries known as data brokers.

Data brokers operate in many forms, but they generally profit from aggregating, packaging, and transferring the personal information of large numbers of individuals. Many of these companies compile nonpublic information such as smartphone geolocation, internet history, communication metadata, utilities, and biometrics, which they obtain from sources like mobile apps and web browsers using software development kits, cookies, real-time bidding processes, and direct purchases. Some also scrape publicly available information like social media posts, audio and visual footage taken in outdoor areas, or government archives like Department of Motor Vehicles records, voter registrations, tax or property filings, or arrest histories.[12] Data brokers may also obtain information from other data brokers or even purchase mobile apps in order to acquire datasets, creating an intricate, nontransparent web that affected individuals and the general public cannot follow.

According to Sensor Tower, the average American interacts with almost 50 mobile apps per device per month, many of which track intimate details such as a person's location history, communications records, purchases, web or browsing activity, and biometrics. When data brokers combine such information from multiple first-party sources, they can paint an extensive picture of a person's lifestyle habits and preferences. A 6(b) study by the Federal Trade Commission (FTC) in 2014 found that Acxiom had over 3,000 data points for almost all U.S.

individuals, and since then the information ecosystem has only grown.[13] The same 6(b) study also found that some of the nine large data brokers surveyed "store all data indefinitely, even if it is later updated, unless otherwise prohibited by contract."[14]

## *Widespread deployment of predictive algorithms across all sectors has generated high demand for personal information.*

There is no single legal definition of a data broker in the United States, which presents a challenge to regulating their interactions with government agencies. In 2014, the FTC described data brokers as "companies that collect consumers' personal information and resell or share that information with others."[15] This definition broadly encompasses both first- and third-party companies, as well as those that transfer data without a monetary transaction.[16] California requires any business that "knowingly collects and sells to third parties the personal information of a consumer with whom the business [it] does not have a direct relationship" to register with the state attorney general.[17] As of November 2022, 515 companies had done so.[18] The American Data Privacy and Protection Act (ADPPA) generally defines third-party collecting entities as those "whose principal source of revenue is derived from processing or transferring the covered data that the covered entity did not collect directly from the individuals."[19] This report primarily analyzes third-party data brokers who lack direct relationships with individuals linked to datasets and fall within the ADPPA's definition.

While some data brokers sell datasets in aggregate form, deidentification does not guarantee individuals' privacy or safety. It is possible to reidentify specific individuals by combining multiple attributes or tracking location data points over an extended period.[20] In 2013, Harvard University professor Latanya Sweeney reidentified over 40 percent of 1,000 "anonymous" individuals who shared DNA for the Personal Genome Project by combining their information with public records like voter registration.[21] Tufts University professor Susan Landau recently testified that often only four data points are required to reidentify specific individuals.[22] In a 2022 letter, a trio of senators expressed concerns that BetterHelp and Talkspace had shared sensitive mental health information that could readily reidentify individuals: "Even though you claim this data is anonymized, it can still provide third parties with important and identifying information."[23] One broker, Fog Data Science, claims it does not collect names or email addresses but sells the long-term geolocation history of smartphone devices, which can infer where somebody lives or sleeps based on their movement patterns.[24] Furthermore, even aggregated location patterns can help law enforcement officers locate abortion facilities with high levels of activity or detect routes along the U.S.-Mexico border with unusual traffic.[25]

Data brokers may also build and license algorithmic models to infer or predict information from otherwise unconnected data points, such as health, finances, race, religion, gender identity, sexual orientation, familial status, and more.[26] Without federal regulations, Americans have little control over how data brokers handle their personal information, particularly since first-party businesses typically do not disclose the identities of the third parties with whom they share such information or how algorithmic inferences can inform decisions that could significantly affect people's lives.

## Examples of U.S. data brokers

- LexisNexis has reportedly compiled over 78 billion data points from 10,000 public and private sources in 442 lifestyle categories that predict individual health risks and subsequent medical costs. While the company stated in 2018 that its analysis had not yet influenced individual insurance costs, there is no guarantee this will not happen in the future.[27]
- As of 2014, an Equifax subsidiary had reportedly aggregated and sold access to employee pay stub information for approximately 38 percent of the U.S. workforce.[28]
- Datalogix compiles and sells personal shopping history from over 1,400 store loyalty programs.[29]
- LexisNexis had reportedly scraped over 37 billion data points from 10,000 different government sources as of 2021, including criminal and property records. Meanwhile, Spokeo, Intelius, and BeenVerified, also known as people search websites, sell access to personal information scraped from public records to anybody on the internet, typically for a low fee.[30]
- SafeGraph, Venntel, X-Mode, and Babel Street purchase geolocation and other personal information from smartphone apps, advertising exchanges, and other data brokers, which they then sell to other companies, individuals, or government agencies. In recent years, U.S. agencies including the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Defense Intelligence Agency (DIA) have purchased U.S. smartphone geolocation information from data brokers without a warrant.[31]
- Clearview AI has reportedly scraped billions of images from publicly available websites, including social media platforms. Using facial recognition technologies, it matches specific individuals to uploaded photos. It licenses access to this extensive database to over 3,000 federal and state entities, including the Central Intelligence Agency (CIA) and FBI.[32]
- Giant Oak, Palantir, and Barbaricum monitor social media platforms in aggregate, allowing customers to search billions of user-generated posts for keywords or images. The DHS has reportedly contracted private vendors to track open-source social media posts to identify individuals within the United States that could be associated with visa overstays, public safety risks, or national security threats.[33] Starting in March 2020, Barbaricum, in partnership with Palantir, received a $2.1-$5.5 million contract to track real-time social media activity, which could include content that users later delete, from Immigration and Customs Enforcement (ICE).[34]
- Vigilant Solutions and Thomson Reuters have monitored and stored the image, location, and time stamp history of billions of license plates in open-air parking lots, highways, and intersections, effectively providing a warrantless means of tracking individuals' locations for thousands of U.S. law enforcement agencies.[35] Between 2017 and 2021, the DHS awarded $7.4 million to West Publishing Corporation, owned by Thomson Reuters, to access its license plate recognition database.
- Fog Data Science has advertised collecting billions of data signals from mobile apps, revealing "near real-time" location histories from over 250 million U.S. devices dating back to 2017. It has sold access to this information to federal, state, and local law enforcement agencies for under $10,000 annually, sometimes offering free trials.[36]

# Privacy Concerns from Domestic Government Relationships with U.S. Data Brokers

By design, third-party data brokers pose risks to a person's privacy. Among other practices, the industry infers intimate details about a person's life from a myriad of data points, processes personal information for secondary purposes outside the scope of the initial interaction, and multiplies the number of parties that access a dataset throughout its life cycle. For instance, ProPublica reports that data brokers have helped health insurers predict physical and mental health conditions by analyzing disparate data points such as education, age, race, marital status, neighborhood, and recent purchases.[37] In addition, Duke University researcher Joanne Kim found that several U.S. data brokers may have access to contact information that can identify individual users of mobile mental health apps.[38]

As a result, privacy violations by the U.S. data brokerage industry can cause both measurable and immeasurable consequences for Americans, including psychological, emotional, reputational, financial, and physical harm. For example, data brokers have targeted predatory advertisements related to debt or financial scams to individuals whom they have algorithmically profiled as financially vulnerable.[39] In 2016, LeapLab settled with the FTC after selling payday loan applications to marketers who then stole money from bank accounts.[40] Data brokers can also reveal details such as sexual orientation without individuals' consent, placing LGBTQ+ individuals at disproportionate risk of doxing or discrimination. In 2021, a senior official of the U.S. Conference of Catholic Bishops resigned after being involuntarily outed by a religious publication that had purchased his Grindr location information from a data broker.[41] Data brokers can even enable stalking or physical violence. In 2020, a gunman shot a federal judge's husband and son after purchasing her home address and other personal information online.[42]

When third-party data brokers share personal attributes with U.S. government agencies, they may influence significant societal decisions, such as imprisonment, deportation, distribution of public benefits, and more. Since 2014, ICE has regularly contracted Palantir to mine personal information from public and private

databases, reportedly facilitating deportations, workplace raids, and family separation.[43] In 2019, ICE–aided by Palantir systems–arrested 680 workers at a food processing company in Mississippi, leaving at least two children at home unaccompanied for over a week after their parents were detained.[44] In 2021, LexisNexis received a contract worth up to $1.2 billion to verify individuals' identities for state unemployment insurance claims, a critical lifeline for many Americans.[45] The same year, researchers at the Center for Democracy and Technology uncovered an additional 30 U.S. federal government awards for data brokerage services that totaled approximately $86 million, likely a fraction of the full scope of government contracts that data brokers received.[46]

As U.S. government agencies become increasingly dependent on the private sector, some analysts point out that data brokers can offer material benefits. For example, the Centers for Medicare and Medicaid Services, Department of Labor, Internal Revenue Service, and Department of Veterans Affairs have used aggregated data points to predict fraudulent or erroneous payments.[47] However, the same datasets used for beneficial purposes can also lead to secondary, more controversial outcomes. For example, Thomson Reuters offers a CLEAR database that contains home addresses, vehicle registrations, employment histories, and utility records from at least 400 million individuals. Although the company markets this database to provide alternative credit histories for people who lack access to traditional credit cards, ICE also reportedly used this service until 2021 to help enforce deportations of individuals who do not pose physical security threats.[48] In fact, data brokers can serve a variety of functions for both public and private organizations, potentially informing decisions related to employment, credit or risk scores, health insurance, public interest research, political outreach, and policing.[49]

Regardless of the purpose behind the surveillance effort, there is at least some ethical ambiguity with any contract that U.S. government agencies sign with data brokers. First of all, U.S. government contracts feed into the rapid growth of an industry that faces minimal legal limitations on collecting, processing, storing, and sharing data. Second, algorithms based on personal attributes sometimes draw inaccurate conclusions that can significantly affect people's lives. Between 2008 and 2019, ICE relied on faulty databases, compiled with the assistance of private data brokers, to arrest approximately two million individuals based on their country of birth and lack of verified citizenship documents–a practice a federal judge found unconstitutional in *Gonzalez v. ICE* (2019).[50] Due to overreliance on flawed electronic databases, law enforcement officers have mistakenly targeted individuals such as Renata and Chris Simmons, whose dog police officers shot, and Denise Green, whom officers wrongly held at gunpoint.[51] In many cases, individuals do not have the option to view these databases or request that data brokers correct inaccurate profiles.

*U.S. government contracts feed into the rapid growth of an industry that faces minimal legal limitations on collecting, processing, storing, and sharing data.*

When data brokers collaborate with law enforcement agencies to implement predictive policing, they could produce inaccurate or flawed outcomes based on historically biased training data. At the local level, some police departments have used modeling systems designed by firms like PredPol to anticipate crime based on historical patterns and adjust their patrol routes accordingly.[52] In addition, data brokers have sold Americans' personal information to state-run fusion centers, which hire analytics firms like Palantir to scan

past data for future threats.[53] But since local governments have historically focused surveillance resources on neighborhoods based on factors like race, income, and religion, predictive modeling systems draw upon and reproduce these biases in future cycles. At the federal level, the DHS's use of social media analysis to predict threats is notoriously defective, since it frequently uses vague keywords as proxies for illegal activity and may fail to identify context clues, cultural differences in speech, and satire.[54]

The data brokerage industry is shadowy and opaque, as companies rarely disclose details of their data collection and analysis to external parties. This lack of transparency prevents government agencies and other customers from discovering potential biases in these technologies, even when they lead to erroneous criminal arrests. Trade secret protections further complicate access to exculpatory evidence that could prove an individual's innocence if inaccurate datasets or algorithms are used.[55] Although data brokers may post vague privacy policies on their websites, they generally do not disclose the specific entities they access information from, clients they share information with, methods of building algorithmic inferences, and types of data that are stored or shared. In other words, there are few ways for impacted individuals, public interest researchers, or the general public to learn about the sale of personal information or to correct any subsequent predictive profiling.

*Since local governments have historically focused surveillance resources on neighborhoods based on factors like race, income, and religion, predictive modeling systems draw upon and reproduce these biases in future cycles.*

Aside from accuracy concerns, data brokers can also perpetuate systemic biases in law enforcement by directly targeting personal attributes like race, ethnicity, country of origin, religion, and income.[56] For example, X-Mode and Predicio have reportedly sold information from smartphone apps like Muslim Pro and Salaat First to Department of Defense (DOD) contractors.[57] Kochava, which is facing an FTC lawsuit, sold location information that could be used to track people who visit places of worship, reproductive health facilities, addiction recovery centers, and homeless shelters.[58] In mid-2020, Mobilewalla reportedly monitored the device geolocation history of approximately 17,000 individuals at Black Lives Matter demonstrations, and the Los Angeles Police Department tested ABTShield to scan Twitter for keywords like "lives matter," "protest," and "solidarity."[59] In 2018, the DOJ initiated an investigation into the Oregon TITAN Fusion Center for tracking local residents who had posted #BlackLivesMatter on social media platforms.[60] Furthermore, Venntel has sold smartphone geolocation data to ICE and U.S. Customs and Border Protection to track individuals along the U.S.-Mexico border, which increases the vulnerability of immigrants and noncitizens.[61]

# National Security Concerns about Foreign Government Access to the U.S. Data Brokerage Ecosystem

In the United States, most private companies, including data brokers, face few constraints on transferring or storing personal information outside the country. As a result, foreign governments can easily obtain sensitive personal information about Americans through data brokers, whether through direct transactions or third-party intermediaries like front companies. However, due to a general lack of transparency, it is difficult to measure the degree to which U.S. data brokers currently work with foreign governments, including China or Russia.

In 2020, William Evanina, then director of the U.S. National Counterintelligence and Security Center, stated that China is "one of the leading collectors of bulk personal data around the globe, using both illegal and legal means."[62] Between 2020 and 2021, the *Washington Post* documented over 300 relationships between China and Chinese-based private data miners to cross-analyze social media posts, public records, and commercial datasets.[63] These included detailed profiles of domestic and foreign journalists and critics, some of whom were located in the United States, that were accessible to China's Propaganda Department, state media, law enforcement, and military.[64] In 2018, China's state-controlled People's Daily reported the government's public opinion data mining industry was worth tens of billions of yuan and rapidly expanding by 50 percent each year.

Although foreign governments, like China, do not have legal jurisdiction over most Americans, they could still benefit from the ubiquitous digital surveillance U.S. data brokers offer. For example, foreign entities could purchase sensitive geolocation information to target specific high-profile individuals like politicians or journalists. Demonstrating the ease of smartphone tracking, the *New York Times* obtained over 50 billion anonymized smartphone geolocation points from 2016 to 2017 and almost instantaneously identified former U.S. president Donald Trump, Secret Service agents, senior congressional staffers, and DOD officials.[65] In addition to geolocation, commercial data sales related to physical or mental health, personal relationships,

or finances could increase the vulnerability of high-profile Americans to blackmail or doxing by foreign and domestic bad actors.[66]

Foreign governments gaining direct access to Americans' personal information or algorithmic inferences through U.S. data brokers could compromise military or intelligence operations.[67] In 2016, PlanetRisk inadvertently detected U.S. military operations in Syria by tracking soldiers' smartphone geolocation data.[68] In December 2017, Strava unveiled a publicly available heat map that displayed over 1.4 trillion latitude and longitude points of individuals wearing fitness trackers, possibly implicating those in military bases in Afghanistan, Syria, Niger, Djibouti, Yemen, and Turkey.[69] As recently as 2021, Acxiom, LexisNexis, and Nielsen actively advertised selling or sharing information related to military officers.[70] Even China cautioned its People's Liberation Army personnel in 2015 about the data protection risks of "device[s] that can record high-definition audio and video, take photos, and process and transmit data"—in other words, most popular consumer products today.[71]

Advanced data analysis could also help foreign actors strategically promote authoritarian or otherwise harmful messaging during U.S. elections based on voters' interests and backgrounds. During the 2016 U.S. presidential election, the Russia-linked Internet Research Agency (IRA) purchased about 3,000 political advertisements and uploaded 80,000 posts on Facebook using stolen U.S. identities, reaching tens of millions of U.S. users.[72] The IRA disproportionately targeted Black voters with both paid advertisements and unpaid content to discourage turnout; many of its user-generated posts mentioned race in some form.[73] A subsequent investigation by the Senate Select Committee on Intelligence, led by Robert Mueller, found the threat posed by ad targeting "is magnified by the ease with which personal data can be purchased or stolen by a foreign adversary with advanced cyber capabilities."[74]

Seven years after the 2016 election cycle, commercial data brokers routinely sell Americans' personal information to U.S. political campaigns, leaving the infrastructure in place for foreign governments to potentially influence domestic elections using the same tools. Both Democratic and Republican campaigns use U.S. data brokers like Experian to purchase datasets on income, religion, gun ownership, credit score, and voter registration in order to direct relevant online advertisements, paper pamphlets, and phone calls to voters. The Republican National Committee reportedly possesses over 3,000 data points per U.S. voting adult.[75] These tactics resemble those used by the controversial UK-based firm Cambridge Analytica, which amassed personal information from over 50 million Facebook users to target advertisements and fundraising requests for Trump's 2016 presidential campaign.[76] The widespread availability of these datasets, combined with common data brokerage practices of categorizing individuals based on inferred background or interests, could facilitate foreign government targeting of disinformation in future democratic elections.

The vast quantity and scope of information that data brokers store also enlarge the attack surface for state-sponsored cyber breaches, especially since not all companies employ adequate security protections.[77] After the Chinese government hacked Equifax in 2017, exposing sensitive information of approximately 147 million Americans, the FTC discovered Equifax had failed to implement basic security measures such as encryption and strong passwords.[78] In 2019, hackers offered up LimeLeads' non-password-protected database for sale online, exposing names, email addresses, and home addresses from 49 million customers.[79] Other major data broker breaches include Acxiom in 2003, Epsilon in 2011, and Experian in 2015, highlighting how U.S. personal information is of high interest to both domestic and foreign hackers.[80] In 2005, a Senate hearing warned that massive aggregation and storage of sensitive personal details could create opportunities for identity theft. Since then, data collection has only escalated.[81]

*Seven years after the 2016 election cycle, commercial data brokers routinely sell Americans' personal information to U.S. political campaigns, leaving the infrastructure in place for foreign governments to potentially influence domestic elections using the same tools.*

Adam Klein, director of the Robert Strauss Center on International Security and Law of the University of Texas at Austin, notes, "As long as this [the data broker] business model persists, it will remain virtually impossible to prevent this information—and the intelligence bounty that it represents—from falling into the hands of hostile foreign powers."[82] Although foreign governments may access information through many channels, the growing data brokerage industry both expands and expedites authoritarian surveillance and censorship efforts to a larger scale.[83] This highlights the importance of modernizing privacy laws to curb extraneous data collection and mitigate risks to privacy, civil rights, and national security across the ecosystem.

# Current U.S. Privacy Laws Fail to Check U.S. Data Broker Partnerships with Government Agencies

## The U.S. Federal and State Commercial Privacy Landscape

The United States has dozens of federal and state statutes that address how private businesses protect personal information, but they have not undergone significant updates in decades and have fallen behind technological advancements. Many U.S. commercial data protection laws cover only specific sectors and types of companies, which leaves certain underregulated entities—data brokers, digital platforms, and mobile apps—free to process, share, and store an extensive range of sensitive personal information.

For example, the federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 generally requires medical providers and health insurers to obtain affirmative express consent before sharing personal health information, but does not apply to data brokers, which can transfer mental or reproductive health data at will.[84] Similarly, the Family Educational Rights and Privacy Act (FERPA) of 1974 requires U.S. schools to follow certain privacy safeguards to protect their students, but does not prevent schools from using data brokers to target recruitment advertisements to individuals who are not enrolled.[85] Most federal laws do not directly address geolocation tracking and sharing, except for the Children's Online Privacy Protection Act (COPPA) of 1998 which requires companies to obtain parental consent before collecting personal information from minors under 13.[86]

Only eight states—California, Utah, Virginia, Colorado, Connecticut, Iowa, Indiana, and Tennessee—have enacted laws that allow residents the right to access, correct, and delete the personal information that private companies, including data brokers, hold.[87] These states also require first-party companies that share information with third parties to impose contractual privacy obligations and mandate various degrees of data minimization. However, most U.S. states have not yet enacted comprehensive privacy laws, and the laws that exist have varying strength. For example, California allows people to opt out of automated profiling, while

Utah does not. In addition, California and Vermont require data brokers to register with the state, providing some degree of transparency for individuals, regulators, and the public.[88] Nevada, meanwhile, mandates data brokers to permit individuals to opt out of the sale or transfer of their personal information.[89]

*Many U.S. commercial data protection laws cover only specific sectors and types of companies, which leaves certain underregulated entities—data brokers, digital platforms, and mobile apps—free to process, share, and store an extensive range of sensitive personal information.*

The FTC can act against companies, including data brokers, engaging in "unfair or deceptive acts or practices" across the U.S. economy, but there are limits to its enforcement power. Historically, it has focused primarily on companies that engage in deceptive behavior or misrepresent their privacy policies, leading to a system of "notice and consent," in which companies require users to click "I accept" to data collection in order to access basic services. But an emphasis on notice and consent can incentivize companies to publish vague language that promises little-to-no privacy protections. As the Information Technology and Innovation Foundation observed in 2015: "If you do not want the FTC to come after you, do the bare-minimum on privacy."[90] As a result, many data brokers, such as Oracle and Epsilon, openly admit to aggregating data from thousands of companies in their privacy policies.[91]

Most agree the traditional notice-and-consent model does not effectively safeguard user privacy or restrict data brokerage practices. Even if individuals click "I consent" to use a first-party mobile app, they have no direct relationship with third-party data brokers and typically cannot control the future resale or use of their personal information. Additionally, nearly all digital platforms share personal information with third parties, leaving individuals with few options but to accept blanket data transfers if they want to engage in fundamental functions such as electronic communications, work, social or political activities, e-commerce, and rideshares.

Reflecting these concerns, the FTC filed a complaint against Kochava in August 2022 to challenge its sale of the geolocation history of hundreds of millions of people, which could reveal visits to sensitive locations like reproductive health clinics or addiction recovery centers. Notably, the FTC argued Kochava's practices are unfair, rather than deceptive, under Section 5 of the FTC Act—a departure from the traditional notice-and-consent approach.[92] In August 2022, the FTC also issued an Advance Notice of Proposed Rulemaking (ANPR) seeking public comment on topics that could directly affect data brokers, including business models "that are premised on or incentivize persistent tracking and surveillance."[93] However, a federal court dismissed the FTC's complaint against Kochava in May 2023, writing that "the alleged privacy intrusion is not sufficiently severe to constitute substantial injury," and the ANPR is not guaranteed success either.[94] The FTC filed an amended complaint against Kochava the following month, but bipartisan FTC commissioners have also recognized the limits of existing enforcement authority and have called on Congress to pass legislation to directly regulate data privacy practices and strengthen agency resources.[95]

## Voluntary and Compelled Disclosure of Personal Information by U.S. Government Agencies

As with commercial privacy laws, Congress has enacted several pre-internet statutes that limit the U.S. government's access to data held by private companies. But Congress has not passed major reforms in years, and the recent evolution of the data brokerage industry has offered government agencies a loophole to work around outdated and uneven rules on digital surveillance.

For example, the Electronic Communications Privacy Act (ECPA) of 1986 prevents certain types of businesses, such as phone companies and internet service providers, from voluntarily disclosing U.S. communications content and metadata to U.S. government agencies without a court order or subpoena. However, the ECPA does not apply to third-party data brokers or app developers, which largely did not exist back in 1986, leaving gaps where phone companies can sell "non-content" personal information to data brokers, who, in turn, can sell to government agencies outside the legal process.[96] In 2018, Senator Ron Wyden called attention to Verizon, AT&T, T-Mobile, and Sprint's sales of customer cell phone geolocation data to companies like LocationSmart, Zumigo, and Securus Technologies, which subsequently sold it to law enforcement agencies.[97] In 2014, the Obama White House recommended modernizing the ECPA to remove "archaic distinctions" in privacy protections, but one decade later, the statute has not been substantially amended.[98]

In the absence of a statutory framework that directly regulates data brokers' sales, U.S. government agencies are still bound by constitutional constraints that provide minimum processes to protect individual privacy and civil liberties. However, technological advancements raise legal uncertainties about the application of data brokerage contracts to traditional legal jurisprudence, especially regarding Fourth Amendment requirements for government agencies to obtain probable cause warrants to conduct "unreasonable searches and seizures." While the Supreme Court has historically defined "unreasonable searches and seizures" as violating a "reasonable expectation of privacy," commercial digital surveillance has eroded societal expectations of privacy over time.[99]

To determine what constitutes a reasonable expectation of privacy, courts have traditionally distinguished between public and private places, generally holding that Americans possess a lesser expectation of privacy in at least some public settings.[100] In line with this traditional viewpoint, Clearview AI reportedly does not require U.S. government agencies to obtain warrants to access its facial recognition database, which draws billions of images from publicly available sources.[101] Similarly, U.S. law enforcement agencies have not obtained warrants before accessing Vigilant Solutions's and Thomson Reuters's vehicle location databases, which automatically scan license plates in public areas.[102] Nor have government agencies sought warrants to scan billions of public social media posts and images for specific keywords or people, aided by analytics companies like Palantir and Giant Oak.[103]

*Technological advancements raise legal uncertainties about the application of data brokerage contracts to traditional legal jurisprudence, especially regarding Fourth Amendment requirements for government agencies to obtain probable cause warrants to conduct "unreasonable searches and seizures."*

The U.S. data brokerage industry also benefits from the third-party doctrine, or a legal notion that people do not possess a reasonable expectation of privacy from government agencies in information that they voluntarily share with third parties.[104] In *Carpenter v. United States* (2018), the Supreme Court rejected the DOJ's argument that the third-party doctrine should extend to cell site location information collected over a seven-day period, pointing out that smartphones are now a de facto requirement for modern society and that individuals cannot voluntarily choose to hand over unlimited geolocation data. However, the *Carpenter* decision was narrow, and it did not "call into question conventional surveillance techniques and tools, such as security cameras" nor "collection techniques involving foreign affairs or national security."[105]

While *Carpenter* leaves a fair amount of gray area on the constitutionality of data brokerage partnerships with U.S. government agencies, these activities have nevertheless continued. In 2021, the DIA stated in a memo that it "does not construe the *Carpenter* decision to require a judicial warrant endorsing purchase or use of commercially-available data for intelligence purposes."[106] In 2020, Chad Mizelle, then acting general counsel at the DHS, arrived at a similar conclusion.[107] The January 2022 ODNI report acknowledged that intelligence agencies have purchased the same types of cell phone geolocation records that *Carpenter* contested, stating that the sensitivity of such data may warrant additional safeguards.[108] Some legal experts, like Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur of the Center for Democracy and Technology, argue that "the broad language of the [*Carpenter*] opinion suggests that the government must also obtain a warrant in order to access sensitive personal information in contexts beyond the facts of the case."[109] Yet others, such as Berkeley Law's Orin Kerr, state that the Fourth Amendment does not require U.S. government agencies to have any justification or warrant to purchase information from a willing seller.[110]

Technological advancements also create legal uncertainties around the constitutionality of geofence warrants. In *United States v. Chatrie* (2022), a Virginia federal court found a geofence warrant identifying all smartphones signed into Google within 150 meters of a bank robbery unconstitutional. The court ruled that law enforcement lacked probable cause to broadly track the geolocation history of every nearby individual during that time frame but, emphasizing the "novel" nature of geofencing technology, allowed the government to proceed with the evidence under the "good faith" exception in *United States v. Leon*.[111] In *United States v. Rhine* (2023), the D.C. District Court upheld the constitutionality of a geofence warrant to track January 6 rioters at the U.S. Capitol but did not address whether the defendant had a reasonable expectation of privacy in his smartphone geolocation history.[112]

Data brokers offer a path to work around these legal uncertainties, allowing law enforcement officers to sidestep geofence warrants by selling similar information (such as devices in specific locations at certain times) in ways that are much broader than a traditional warrant might allow. The judicial branch alone cannot resolve these legal issues. While courts interpret existing legal frameworks, they do not create new ones; rather they often either address overarching concepts like the Fourth Amendment or issue specific rulings like in *Carpenter*. Hence, Congress must act to both establish new privacy safeguards and amend existing statutes to account for emerging technologies.

# The Commercial and Government Surveillance Ecosystem in the European Union and China

Advancements in data collection have exacerbated geopolitical tensions. It is difficult to preserve global trust if too many governments are escalating their own intelligence activities while also being averse to surveillance by other nations. Individuals and multinational companies, in turn, bear the immediate consequences of this lack of trust, especially if governments respond to extraterritorial access to personal information by cutting off cross-border exchanges of information and commerce.

Most large economies like the European Union, Canada, and China have enacted national laws that regulate how technology platforms collect, process, and share personal information. The United States, which does not have a comprehensive federal commercial privacy law, is an outlier. Despite this, all four governments have acted as customers as well as regulators of commercial data brokers, though the size of the industry in each country varies widely. In December 2022, the Organization for Economic Cooperation and Development (OECD) released nonbinding principles in the Declaration on Government Access to Personal Data Held by Private Sector Entities, in which 38 OECD countries pledged to follow democratic practices like transparency, accountability, and redress when compelling access to private sector data.[113] The guidelines acknowledged, but did not specifically address, stakeholder calls for multilateral engagement on voluntary government access to commercial or publicly available personal information.

*It is difficult to preserve global trust if too many governments are escalating their own intelligence activities while also being averse to surveillance by other nations.*

If the United States can demonstrate willingness to implement major domestic restrictions on commercial data broker purchases, there is significant opportunity to illustrate shared values on privacy and promote global trust in cross-border data flows. As the data brokerage industry continues to operate globally, it is also important to understand how non-U.S. governments procure commercial datasets and explore ways to promote consistent and interoperable global frameworks.

## Constraints on the EU Data Brokerage Market under the General Data Protection Regulation

Under the General Data Protection Regulation (GDPR), data brokers face stricter legal constraints in the European Union than in the United States. The data brokerage market exists in the European Union, but on a smaller scale. The EU market is estimated to be around €100 billion ($116 billion) compared to a U.S. market of over $200 billion.[114] Around 2018, Privacy International exercised its GDPR right to access data held by several major U.S.-based data brokers like Acxiom, Oracle, and Equifax, ultimately filing complaints to UK and EU data protection authorities over alleged violations of GDPR provisions on purpose limitations, consent, transparency, and more.[115] The UK Information Commissioner's Office subsequently audited several major data brokers, including Acxiom, Data Locator Group, GB Group, Experian, Equifax, and Callcredit. Around the same time, France's Commission Nationale de l'Informatique et des Libertés (CNIL) audited over 50 data brokers and ad-tech companies.[116]

In 2020, the Norwegian Data Protection Authority fined Grindr €6.5 million ($7.1 million) for sharing personal information, including geolocation, age, gender, and sexual orientation, with third-party marketing entities between at least 2018 and 2020 without a valid consent mechanism.[117] The same year, the Privacy Collective and others filed a class action lawsuit for €11 billion ($12 billion) against Oracle and Salesforce in the Netherlands, alleging that their use of ad-tech trackers and real-time bidding systems violated the GDPR.[118] The Privacy Collective's suit was dismissed for lack of standing, but future litigation is possible.[119] In 2022, the French CNIL fined Clearview AI €20 million ($22 million) for scraping EU personal information in violation of the GDPR, following previous charges by data protection authorities in Italy, Greece, and the United Kingdom.[120] In other words, the GDPR's transparency and data minimization requirements expose EU data brokers to heavier compliance costs and higher possibilities of litigation, making the industry riskier and less profitable than in the United States.

Since 2018, the GDPR has established legal responsibilities for most public and private sector entities, including data brokers, that process information "relating to an identified or identifiable natural person." The GDPR applies to some types of pseudonymized information, or information that "can no longer be attributed to a specific data subject," and primarily excludes datasets where individuals cannot possibly be identified or reidentified in the future.[121] In addition, GDPR protections cover public records and publicly available information.[122] Overall, the GDPR regulates a much broader swath of personal information than what most recent U.S. legislative measures propose (see Section VII), which can constrain how EU data brokers initially collect and store commercial datasets, social media analysis, and public surveillance imagery.

Although the GDPR does not directly apply to most law enforcement and intelligence operations, it still requires data brokers to have legal justification to sell personal information to government agencies—unlike the U.S. system, which places few hard restrictions on voluntary disclosure. Article 6 of the GDPR allows covered entities to process data to "protect the vital interests of the data subject or of another natural person" and perform "task[s] carried out in the public interest." Article 23 of the GDPR allows member states to pass

legislation to restrict the GDPR for national security, defense, and other "important objectives of general public interest." The GDPR's purpose limitations prevent entities from collecting personal information for one reason, such as to provide a requested service, but then using it for secondary purposes, such as selling it to law enforcement through data brokers, without an additional legitimate reason. Nonetheless, the permitted categories are broad, so law enforcement agencies overall can still purchase commercial datasets.[123]

In addition to purpose limitations, Article 5 of the GDPR requires data brokers to process personal information "fairly and in a transparent manner" and grants individuals the rights to access, correct, and delete data after they are processed. Article 14 requires data processors to disclose the names or categories of recipients of personal information, which could increase visibility into third-party data transfers. Furthermore, Article 22 allows individuals to opt out of automated profiling that could "significantly" affect them, which could limit some data brokerage activities but does not entirely prohibit behavioral advertising.[124] Article 35 mandates entities perform "data protection impact assessment[s]" for processing activities "likely to result in a high risk to the rights and freedoms of natural persons," which could affect development of tools by third-party data brokers for law enforcement or intelligence use.

Although the GDPR has reduced the potential for privacy risks stemming from the EU data brokerage industry, it has not eliminated them entirely. For instance, OnAudience identified 1.4 million people who had searched for LGBTQ+ rights content ahead of the 2019 Polish parliamentary election, according to the Irish Council for Civil Liberties. While the data broker claimed its objective was to target voters with information about pro-equality campaigns, any data breaches or secondary uses of highly sensitive information like sexual orientation or gender identity could potentially result in involuntary outing or discrimination.[125] The GDPR has also experienced challenges in enforcement timing and funding, both at the international and national levels.[126] As of March 2022, Ireland's Data Protection Authority had resolved only around 65 percent of cases involving cross-border data transfers since the GDPR became effective in 2018.[127] In addition, the European Data Protection Board (EDPB) and national-level data protection authorities (DPAs) have faced procedural and communications challenges with regulatory enforcement.[128]

*Although the GDPR has reduced the potential for privacy risks stemming from the EU data brokerage industry, it has not eliminated them entirely.*

## Efforts toward Member State Harmonization on Law Enforcement and Privacy

Despite the constraints the GDPR imposes on the data brokerage industry, some EU member states have continued to purchase commercial datasets and automated open-source intelligence from private vendors, raising privacy concerns. In 2022, the Dutch supervisory committee Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD) revealed the country's intelligence agencies Algemene Inlichtingen- en Veiligheidsdienst (AIVD) and Militaire Inlichtingen- en Veiligheidsdienst (MIVD) had contracted private companies to analyze commercially available personal information and automatically scan open-source

information.[129] However, a general lack of transparency across EU intelligence and national security agencies means the full extent of their data broker partnerships is not publicly known, similar to the ongoing situation in the U.S. market.[130]

Article 4(2) of the Treaty Establishing the European Union (TEU) states that "national security remains the sole responsibility of each Member State," though EU law generally overrides any conflicts with national law. Some EU member states have enacted statutes that affect data brokerage relationships. For example, Articles 21 and 41 of the Dutch Intelligence and Security Services Act, or Wet op de inlichtingen- en veiligheidsdiensten (WIV), require authorities to receive permission to engage in the systematic collection of publicly available information, including commercially available datasets.[131] Nonetheless, since the European Union primarily leaves intelligence and law enforcement operations to individual nations, local rules around government transactions with commercial data brokers are fragmented and not always publicly clear. Still, attempts to standardize EU-wide safeguards for civil liberties and national security, such as the European Convention on Human Rights (ECHR), Charter of Fundamental Rights (CFR), Convention 108, and the Law Enforcement Directive, carry implications for the regional data brokerage market.

Article 8 of the CFR affirms individuals' rights to personal data protection in the European Union, stating that processing should take place only with a person's consent or "some other legitimate basis laid down by law."[132] Furthermore, Article 8 of the ECHR prohibits government entities from interfering with a person's "private and family life" except when "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[133] But it is not always possible to draw a clear line at "necessary" or "democratic" in the context of government transactions with commercial data brokers, especially when balancing civil liberties and national security interests. Although the CFR and ECHR—unlike the U.S. Constitution—explicitly recognize privacy as a fundamental human right, the application of traditional rights to new technological developments remains ambiguous.

The Council of Europe, an international organization with 46 countries including 27 EU member states, amended its treaty on individual privacy and data processing in 2018. Article 11.3 of the Council of Europe's amended Convention 108+ states that personal information may be processed for national security or defense activities only "by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society." Article 6 states that more sensitive categories of data—genetic information, criminal history, race, and health information—may be processed only with appropriate legal safeguards.[134] But Article 11 permits data processing for broad categories, including "the prevention of threats to national security and public safety," which do not clearly define EU government restrictions on access to datasets voluntarily sold by third-party brokers.[135]

*It is not always possible to draw a clear line at "necessary" or "democratic" in the context of government transactions with commercial data brokers, especially when balancing civil liberties and national security interests.*

The European Union's Law Enforcement Directive (LED) also sets out requirements for authorities to process personal information in a "lawful, fair and transparent" manner that "constitutes a necessary and proportionate measure in a democratic society."[136] Article 8 of the LED allows data processing to occur only when necessary, based on existing law, and for a legitimate purpose. Article 11 prohibits the use of automated profiling for "adverse" legal decisions without robust safeguards. However, the LED generally does not apply to intelligence authorities and, as such, does not protect individuals from all types of commercial transactions with third-party data brokers.[137]

The European Union has debated the acceptable parameters of facial recognition for law enforcement purposes, including in the context of commercial databases like Clearview AI. In April 2021, the European Commission presented a draft Artificial Intelligence (AI) Act that seeks to prohibit the use of real-time facial recognition in public spaces by law enforcement, except when strictly necessary to mitigate physical threats, prosecute criminal offenses, or locate missing victims.[138] Due, in part, to concerns over the broad scope of these exceptions, the European Council approved an amended version in December 2022 that proposed to ban "remote biometric identification systems that are or may be used in publicly or privately accessible spaces, both offline and online."[139] This update expands the proposed prohibition from real-time surveillance to ex post identification, which would directly affect firms like Clearview AI that rely on ex post facial recognition.[140] Once the AI Act is finalized and enacted, it will become one of the world's first major AI regulations and could carry implications for data brokers that sell facial imagery in not only the European Union but the United States as well.

## *Schrems II* and GDPR Data Adequacy: How Data Brokers Could Create Uncertainty for Cross-Border Data Flows

In *Schrems I* and *II*, the CJEU invalidated the Safe Harbor and Privacy Shield data transfer agreements between the European Union and United States due to concerns that U.S. government surveillance practices did not meet the necessity and proportionality standards required by EU law. In particular, the CJEU cited the U.S. government's ability to conduct bulk surveillance of EU individuals under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333. In response, the Biden administration released a new EU-U.S. Data Privacy Framework (EU-U.S. DPF) in October 2022 that directly adopted the same necessity and proportionality language found in the CFR, Convention 108+, and LED.[141] The EU-U.S. DPF also creates a new redress mechanism to allow individuals within designated countries to request review of suspected U.S. government signals intelligence collection by the ODNI, subject to the oversight of a new Data Protection Review Court within the DOJ.[142] However, the EU-U.S. DPF remains susceptible to future court challenges, and the United States still lacks comparable commercial privacy laws and has not received an adequacy determination under the GDPR.

Going forward, it will be interesting to see whether EU courts and data protection authorities will shift their focus to the growing data brokerage industry in the United States, especially as technological advancements in the private sector continue to enhance U.S. government surveillance. The European Union's transactions with commercial data brokers pose a challenge to mitigating similar U.S. practices, as it is difficult to place geopolitical pressure on other countries to refrain from voluntary data access when the full scope of engagement on both sides is unknown. Fragmented intelligence statutes between EU member states can lead to less robust oversight of government purchases of personal information or algorithmic inferences, even if the GDPR reduces the availability of those commercial datasets overall.

The European Commission has deemed Canada's level of data protection, but not the United States', as "essentially equivalent" to the European Union's, allowing Canada-EU cross-border data transfers greater legal certainty under Article 45 of the GDPR.[143] However, like the United States, Canada has accessed commercial or publicly available information from data brokers and is a member of the Five Eyes alliance. Canada's Criminal Code generally requires domestic law enforcement agencies to receive authorization to access personal information, but their interactions with data brokers are not publicly clear.[144] In a 2019 annual report, the Canadian National Security and Intelligence Review Agency found that the Canadian Security Intelligence Service used publicly available geolocation data without a warrant, even though it "lacked the policies or procedures" to ensure the legality of such access.[145] The Security Intelligence Service and the Communications Security Establishment of Canada, the nation's other major national security agency, both adhere to lighter due process requirements in their respective statutes compared to in the Criminal Code.[146]

*It is difficult to place geopolitical pressure on other countries to refrain from voluntary data access when the full scope of engagement on both sides is unknown.*

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) governs how private companies process and share information, which limits but does not fully prevent commercial transactions with data brokers. After the PIPEDA became effective in 2004, at least one broker, R. L. Polk Canada Inc., announced it would no longer process personal information in Canada.[147] Clearview AI also terminated its services with the Royal Canadian Mounted Police in July 2020 after the Office of the Privacy Commissioner began investigating whether its use violated the PIPEDA and Privacy Act.[148] However, the PIPEDA does not cover de-identified information and still allows firms like Cornerstone, Acxiom, Oracle Canada, Conway, Epsilon Data Management, and InfoCanada to engage in direct marketing or commercial data sharing.[149] Section 7(3) of PIPEDA even allows private entities to voluntarily share personal information with law enforcement agencies without notifying or obtaining consent from the affected person.[150]

Even if the EU's *Schrems I* and *II* and GDPR adequacy decisions have not focused on the relationship between data brokers and government agencies, multilateral dialogues or consensus on safeguards and privacy principles could help improve trust between partner nations like the United States and Canada. All three governments have laid down some guardrails for compelled disclosure of data, but voluntary access to commercial or public information generally has not received the same level of attention or legal protections.

## China's Data Protection and Data Localization Landscape

China's surveillance apparatus relies heavily on private companies that collect and process personal information from both Chinese and non-Chinese individuals. Several statutes codify this relationship, giving China extensive control over the information companies store under its jurisdiction. In response to concerns over China's data localization and national security laws, the United States, European Union, Canada, and other nations have blocked TikTok on government-issued devices.[151] In May 2023, Montana became to first state to issue a blanket ban on all TikTok operations and app downloads within state borders, which, pending legal challenges, will come into effect in January 2024.[152] Because TikTok's parent company, ByteDance, is

based in China, legislators fear the CCP could access information about U.S. individuals that mobile apps, specifically TikTok, transfer or store within Chinese borders. There is no clear public evidence of direct CCP access through TikTok to date, but legislators have generally cited China's 2017 National Intelligence Law, which requires individuals and organizations to "support, assist, and cooperate with state intelligence work according to law," as a primary risk factor.[153]

In addition to the National Intelligence Law, China's Cybersecurity Law requires internet platforms that operate within its national borders to assist law enforcement in identifying content "endangering national security, national honor, and national interests."[154] These categories are fairly expansive. The Cybersecurity Law also imposes explicit data localization requirements, forcing companies to store "personal information or important data" collected in China on domestic servers. Some U.S. technology platforms ceased operations in China after the statute became effective in 2017, but others changed their policies to store data and decryption keys on local state-owned servers.[155] The updated Multi-Level Protection Scheme (MLPS 2.0) also allows the government to monitor domestic private networks for national security threats, facilitating access to all data stored on servers or transmitted on networks within China.

Enacted in June 2021, the Data Security Law (DSL) further strengthens government access to user data, allowing law enforcement to compel private businesses that operate within China to disclose personal information. The DSL broadly defines key terms such as "core data" and "important data," which gives authorities oversight over a range of user data like geolocation, browsing activity, financial records, and communications. For example, "core data," which receives the greatest protections, refers to information that relates to significant public interests, national or economic security, or citizens' welfare. Data localization laws present privacy concerns for individuals located within the United States that communicate with those in China, as government agencies could potentially read cross-border electronic communications stored in local data centers. This legal framework, in parallel with the burgeoning U.S. and Chinese data brokerage industries, gives the Chinese government significant resources to surveil individuals both within and outside of China.

Beyond legal authority to compel disclosure of personal information, the CCP has additionally shifted to contracting private companies that voluntarily sell datasets or analytics software to surveil citizens. China's Ministry of Public Security has reportedly allocated billions of dollars to private sector surveillance technologies under the SkyNet and Sharp Eyes plans.[156] Among these are AI start-ups SenseTime and CloudWalk, which developed facial recognition systems that could identify members of the Uyghur community.[157] According to procurement documents, Wuhan law enforcement has sought out commercial tools to identify people in public spaces, along with their internet, phone, and location history.[158] Shanghai law enforcement, meanwhile, hired Shanghai Cloud Link and other firms to analyze posts and photos from Twitter and Facebook, reportedly combining commercial or public-facing data with government records like driver and voter registries to identify anonymous online accounts.[159]

In 2019, Forbes reported that some Chinese data brokers sold access to personal information online to any willing buyer, not just government entities, for a few dollars.[160] It is not clear how enactment of the Personal Information Protection Law (PIPL) in 2021 will affect the Chinese data brokerage industry. The PIPL, which includes provisions similar to those of the GDPR, requires private companies to process sensitive personal information only when necessary for approved purposes and limit data retention.[161] It also mandates companies obtain individuals' consent to process sensitive personal information, which includes data that could harm "personal dignity" or "personal or property safety."[162] It requires companies that use personal information to conduct algorithmic decisionmaking to follow transparency measures, conduct impact

assessments, and allow individuals to opt out of targeted ads or solely automated decisions. Although the DSL and Cybersecurity Law allow government access to private sector datasets, these provisions could reduce the amount of information first-party platforms and data brokers process within China to begin with, depending on compliance and enforcement in practice.[163]

*Beyond legal authority to compel disclosure of personal information, the CCP has additionally shifted to contracting private companies that voluntarily sell datasets or analytics software to surveil citizens.*

While U.S. due process requirements under the Fourth Amendment and the ECPA are outdated, they generally provide stronger civil liberties protections than Chinese government agencies follow when compelling personal information from private companies. However, the relative strength of U.S. protections becomes less relevant if law enforcement agencies can bypass them by purchasing commercial data from brokers. Voluntary disclosure creates a significant gap the United States could close to strengthen civil and human rights, promote the long-term sustainability of cross-border data flows, and strengthen geopolitical alliances. Without stronger protections for uncompelled access to commercial datasets, it is more challenging for the United States to discourage other countries from engaging in similar practices and to distinguish itself as a global leader in human rights values.

# Recent U.S. Legislative Developments

## Federal Commercial Privacy Legislation

Over the past few years, Congress has proposed dozens of bills that aim to limit data collection, retention, and transfers in the private sector. Some examples include the ADPPA, Consumer Online Privacy Rights Act (COPRA), and SAFE DATA Act, all of which propose a baseline for data minimization, or general limits on companies to collect, process, and share personal data only as necessary to provide a user service or fulfill approved purposes such as fraud or malware detection.[164] Most proposals to update commercial privacy standards would also grant U.S. individuals the right to access, request, and delete personal information held by private companies, as EU individuals possess under the GDPR. These proposals could prevent both first- and third-parties from collecting extraneous data solely for the purpose of resale or targeted advertising and require them to obtain affirmative consent to transfer data to additional parties.

Many major bills in the 116th and 117th Congresses excluded de-identified, aggregated, and publicly available data from their protections. However, as previously discussed, data brokers often collect and package such data or sell inferred insights in aggregate form, so these bills could exempt some business practices that pose privacy problems. In addition, there is ongoing debate over which data processing purposes should be either categorically or conditionally permitted. For example, the California Privacy Rights Act, but not the ADPPA, explicitly allows companies to process personal information for advertising or marketing services and analytic services, provided that the data are "reasonably necessary and proportionate" to the original purpose of collection.[165] Federal commercial privacy legislation could indirectly reduce the amount of personal information available for domestic government agencies to purchase from brokers, but would not directly impose new restrictions for those that wish to do so.

## Proposals to Modernize Government Access to Personal Data

Compared to its commercial privacy legislation efforts, Congress has introduced a smaller range of bills aimed at restricting the U.S. government from purchasing datasets from commercial brokers. The Fourth Amendment Is Not For Sale Act, introduced in 2021, is the most high-profile such initiative to date.[166] The bill's premise was fairly straightforward: if laws like the ECPA or FISA would otherwise require U.S. government agencies to obtain a warrant or court order to compel traditional communications service providers to disclose Americans' data, the same legal procedures should be mandated to purchase that information from a data broker.

The Fourth Amendment Is Not For Sale Act would not apply to all transfers between data brokers and U.S. government agencies, including those that lack an exchange of money or "anything of value." It also would not protect non-U.S. individuals from the sale of personal information to U.S. intelligence or law enforcement agencies. Moreover, depending on interpretation, the bill's definition of "covered customer or subscriber record" could exclude some types of personal information, such as biometrics, algorithmic inferences, publicly available data, or data relating to individuals who are not direct customers of a service. It prohibits government agencies from purchasing "illegitimately obtained information," which companies obtain either deceptively or in violation of terms of service agreements. This could prevent some, but not all, transactions, especially since many privacy policies openly disclose (in vague terms) transfers of personal information to third parties.

*Federal commercial privacy legislation could indirectly reduce the amount of personal information available for domestic government agencies to purchase from brokers, but would not directly impose new restrictions for those that wish to do so.*

While the Fourth Amendment Is Not For Sale Act focuses on the sale of information to the U.S. government, several export control bills emerged in the 117th Congress that would block U.S. data brokers from selling certain categories of personal information to specific foreign governments. The Protecting Military Servicemembers' Data Act aimed to prohibit data brokers from selling personal information related to military personnel to countries like China, Russia, and Iran.[167] In addition, the Protecting Americans' Data from Foreign Surveillance Act, reintroduced in June 2023, would prevent private businesses from transferring sensitive U.S. personal information to certain countries such as China and create a list of low-risk countries where data can flow freely.[168]

In the 118th Congress, legislators have proposed several bills in response to concerns that the CCP could compel ByteDance to hand over TikTok data or control of its content moderation algorithm. For example, the reintroduced ANTI-SOCIAL CCP Act would direct the president to block social media companies, namely TikTok, that use certain algorithms and are located in a handful of countries, including China.[169] The DATA Act would amend the International Emergency Economic Powers Act to allow restrictions on free flows of sensitive

personal information, paving the way for the United States to ban TikTok or future Chinese companies.[170] Also motivated by TikTok, the RESTRICT Act would direct the secretary of commerce to identify and potentially prohibit technology transactions relating to companies under the jurisdiction of six countries including China.[171] The White House has endorsed the RESTRICT Act, even though it could further disrupt international data flows by creating another global adequacy system alongside the GDPR and the PIPL.[172]

# Next Steps to Regulate U.S. Data Brokers and Their Interactions with Government Agencies

Because the U.S. data brokerage industry poses systemic risks to privacy and national security, it requires a comprehensive approach to rein in excessive data transfers across the ecosystem. Without across-the-board rules on how all U.S. mobile apps and data brokers transfer sensitive personal information, banning or divesting any single company, like TikTok, would not effectively prevent data leakage to foreign governments like the CCP. It is also worth noting that neither a divestiture nor forced data localization would stop U.S. domestic agencies from accessing Americans' sensitive personal information—whether through TikTok or data brokers—in ways that could significantly impact privacy and civil liberties.

Instead, the United States needs a multifaceted strategy that (a) imposes boundaries on how all U.S. companies process personal information, (b) places guardrails on U.S. government transactions with data brokers, (c) enforces purpose limitations on data transfers both within and outside the United States, while also protecting cross-border data flows, and (d) improves transparency and grants both regulators and individuals greater control over personal information. As Thorsten Wetzling and Charlotte Dietrich observe, the German Federal Constitutional Court, or the Bundesverfassungsgericht (BVerfG), put forward a double-door model in 2012 that demonstrated privacy safeguards on both sides of the data transfer relationship—the private sector seller and government buyer.[173] In a similar fashion, both U.S. data brokers and government agencies now require greater accountability in a modern digital age. While Congress could implement some data privacy regulations in the short term, it is also important to consider broader open questions—such as the balance between safeguarding publicly available information, cross-border data flows, and free and open expression—that may require additional dialogue and research in the long term.

## Short-Term Actions: Boundaries on Data Brokers

***Federal comprehensive privacy legislation is necessary to regulate how all U.S. businesses, including data brokers, treat personal information.***

The growth of the U.S. data brokerage industry is a result of an outdated privacy legal system that urgently needs modernization to keep up with more than 100 nations, including EU member states, Canada, and China, that have already established nationwide rules for how digital platforms process personal data. As a baseline, any forthcoming commercial privacy legislation should limit first- and third-party companies to collecting, storing, and transferring personal data only as necessary to offer a product that users explicitly request—and delete that information once the transaction or service is completed. This general rule should apply to both original data points and any related algorithmic inferences, including aggregate data that could potentially reidentify individuals or pose substantial privacy risks. In addition, such limitations on processing, retention, and transfers should apply to personal information that is widely accessible on the internet or through other means in cases where an individual's right to privacy outweighs any public interest in that data.

All U.S. companies need clear rules on handling information, but commercial data brokers require enhanced transparency and oversight measures.[174] Congress should require data brokers in all 50 states to register with the FTC, similar to existing provisions in California and Vermont. In turn, the FTC should create a Do Not Track portal to allow individuals to opt out of all data brokerage transfers in a single place. This concept has already been proposed in various forms, dating back to an FTC preliminary staff report on consumer privacy (2010), a Government Accountability Office report on information resellers (2012), an FTC report on data broker transparency (2014), the draft Consumer Data Protection Act (2018), the Data Broker Accountability and Transparency Act (2020), the SAFE DATA Act (2021), and most recently the ADPPA.[175] The FTC already maintains a Do Not Call registry as a centralized portal for individuals to opt out of telemarketing calls, and a Do Not Track portal would be a logical extension of this concept.[176]

Finally, all digital platforms should publicly disclose the specific names of third parties they transfer personal information to, along with the third parties' contact information, categories of data involved, and general purposes of transfer. Such disclosures could bring clarity to otherwise opaque data brokerage practices. Additionally, all individuals should have the right to understand how their personal information is processed and request to correct or delete it. Even if most internet users do not read privacy policies (and should not have to), more detailed public statements could benefit watchdog organizations and regulators, like the FTC, which have used terms and conditions to identify unfair or deceptive acts or practices under the FTC Act.[177]

***Any forthcoming legislation should carefully craft a definition of "data broker" that extends beyond commercial transactions.***

Data brokers operate under many different business models. The legal definition of a data broker is critical because it will determine which specific entities would be subject to any enhanced transparency or accountability requirements, like the registration and opt-out mechanisms proposed here. While some proposed frameworks like the Fourth Amendment Is Not For Sale Act focus on transactions involving money or other resources of value, data brokers can operate outside traditional financial exchanges. Kochava and Clearview AI, for example, have offered free trials or demos of individuals' real-time location information and facial recognition photos, respectively.[178] Data brokers could also voluntarily disclose sensitive personal information to law enforcement agencies without a tangible exchange in hopes of gaining future political goodwill or even to advance their own ideological beliefs—for example, opposition to immigration or abortion.

The FTC's 2014 definition of data brokers as "companies that collect consumers' personal information and resell or share that information with others" can serve as a possible model for data sharing that may or may not involve an exchange of anything of value.[179] However, as data collection and aggregation techniques continue to evolve, it will become crucial to monitor trends in the broader data brokerage industry and periodically revise legal terms as necessary.

## Short-Term Actions: Boundaries on Government Agencies

***Congress needs to pass clear rules to govern how U.S. government agencies procure information from private sector entities.***

Because Congress has not significantly updated the U.S. privacy legal framework in decades, there is a significant amount of legal uncertainty over the application of traditional statutes to advanced commercial surveillance methods. To bridge these gaps, Congress should prioritize additional research into U.S. government commercial transactions with data brokers and ultimately establish bright-line rules to mitigate the potential for privacy or civil liberties abuses. Unless and until robust legal processes are in place, U.S. government agencies should either impose a temporary moratorium or voluntarily obtain a warrant in order to conduct transactions with data brokers, scrape photos or keywords from publicly available sources, and use facial recognition technologies on commercial databases.

***U.S. government agencies must improve public transparency and oversight around data access practices.***

The Obama administration took some measures to improve transparency following the Snowden disclosures, including by declassifying some redacted documents related to FISA surveillance and participating in public hearings.[180] But, in general, the covert nature of national security and law enforcement operations means most Americans are not notified of government surveillance, and many data brokerage transactions may not be disclosed to the public. The January 2022 ODNI report revealed that even "the IC does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements," demonstrating an absence of internal accountability mechanisms as well.[181] The United States is currently undergoing a serious reckoning about racial profiling in state and local law enforcement partially due to increased public visibility, as bystanders can capture videos in public areas using their smartphones and many local police officers wear body cameras.[182] Because many federal operations lack similar external and internal transparency, it is more challenging to exert public pressure to implement critical changes that could benefit society.

Members of Congress previously introduced the Government Surveillance Transparency Act, which would lift most nondisclosure orders issued to technology companies after the surveillance period ends, and the NDO Fairness Act, which would establish necessity requirements to obtain gag orders and limit their duration to 60 days.[183] The NDO Fairness Act, which passed the House of Representatives in 2022, would also require the DOJ to annually report the quantity and acceptance rates of nondisclosure order applications, as well as the number of individuals affected.[184] To further enhance transparency, after an investigation concludes, federal agencies should directly notify all identifiable individuals whose sensitive commercial data (such as precise geolocation, communications, and biometrics) were obtained, with limited exceptions where disclosure might reasonably and significantly impact national security.

The Office of the Director of National Intelligence releases the annual *Statistical Transparency Report Regarding Use of National Security Surveillance Authorities*, which provides generalized figures on the use of compelled mechanisms, including FISA and national security letters.[185] As a next step, all federal agencies could release

annual transparency and equity reports that describe any voluntary procurement of commercial datasets or algorithmic insights from private data brokers. At a minimum, these disclosures should include high-level statistics on the frequency, purpose, and context of data brokerage transactions; the specific identities and contact information of sellers; demographic trends within purchased datasets; and percentage of data access requests that contribute to adverse actions like an arrest. By increasing transparency, it is possible to strengthen public accountability for potential abuses of power or gratuitous access to sensitive personal information, inaccurate or discriminatory outcomes, and disparate impact on historically marginalized communities.

***The FTC and the Privacy and Civil Liberties Oversight Board need sufficient resources to carry out enforcement and oversight duties.***

Although the FTC has decades-long expertise in data privacy and consumer protection, resource constraints may force it to make tough choices between litigating, settling, and passing over cases.[186] In 2019, the FTC had around 1,100 full-time employees to oversee consumer protection across the entire economy, with only about 50 focused on data privacy. In comparison, the UK Information Commissioner's Office had around 700 employees exclusively dedicated to data protection, despite having a smaller data brokerage market, a GDP approximately one-tenth the size of the United States, and one-fifth the U.S. population.[187] As the U.S. digital economy continues to grow, FTC appropriations must similarly increase to help prioritize unfair and deceptive data practices or potentially enforce any future federal comprehensive privacy law. In addition, the agency could benefit from additional funding to conduct 6(b) studies on the effects of data brokers on competition in digital markets, especially for small- or medium-sized businesses that might not possess the data aggregation capabilities of dominant digital platforms.

The Privacy and Civil Liberties Oversight Board (PCLOB) was created to oversee federal government surveillance for counterterrorism purposes, but it may be necessary to strengthen its role and resources to monitor commercial data brokerage transactions as well. The Electronic Privacy Information Center recently called on the PCLOB to examine the use of facial recognition technologies, data-driven fusion centers, and geolocation history from commercial data brokers.[188] The PCLOB could also probe government contracts for social media analysis by private data miners. In addition, the board should prioritize oversight into any potential disparate impact of surveillance on marginalized communities. In 2020, U.S. representatives Anna Eshoo (D-CA), Bobby Rush (D-IL), and Ron Wyden (D-OR) asked the board to investigate federal government surveillance of Black Lives Matter racial equity protests across the United States.[189]

## Short-Term Actions: Boundaries on both Data Brokers and Government Agencies

***While purpose limitations may be effective for private companies, U.S. government agencies need boundaries on their access to personal information in all contexts—no matter their perceived legitimacy of use.***

Data minimization is a core principle of commercial privacy; businesses should collect, retain, and share personal information only if necessary to provide a requested product or service. However, most privacy frameworks also recognize that businesses may need to process personal information for other legitimate reasons, such as to prevent cybersecurity breaches, detect harmful or illegal activities, or issue product recalls. While the GDPR's legal bases for companies to process personal information are broad (for example, with

individual consent, to carry out "legitimate" or "vital" interests, or to fulfill a "public task"), they still establish a basic structure of categorically or conditionally permitted data processing uses that could serve as a general model for other privacy frameworks.

Purpose limitations could be effective in the context of the consumer-business relationship, but U.S. government agencies need hard rules like modernized warrant requirements to govern their access to personal information—regardless of the context or original basis for data collection. The U.S. government should not unduly compromise privacy and civil liberties, even if it aims to address a legitimate national security threat. This is particularly important given the sheer scale of data brokerage: some firms advertise access to billions of data points, and most inevitably relate to individuals who do not pose any public safety risks. In addition to warrant requirements, government agencies need clear data retention and minimization rules to prevent unlimited secondary uses or transfers of Americans' personal information, particularly geolocation, biometrics, and communications.

***Both companies and government agencies should follow specific legal processes to prevent biased or discriminatory outcomes stemming from digital surveillance.***

Since historically marginalized communities have borne disproportionate consequences of surveillance, data brokers need formal procedures to promote civil and human rights. Just as medical and legal professionals have legal obligations to maintain client confidentiality, technology companies should bear duties to safeguard the equity, fairness, and security of their data processing and algorithmic outcomes—no matter if they develop or simply deploy the software. The United States has a body of federal and state civil rights law that prohibits some types of discrimination in specific contexts like employment, credit, or housing, but there is legal uncertainty around how pre-internet statutes apply to data brokerage activities.[190] Therefore, Congress must explicitly recognize privacy as a fundamental civil and human right: no company should use or transfer data in ways that could create disparate impact or unequal digital participation based on factors like race, gender identity, country of origin, religion, sexual orientation, age, or disability status.[191]

There are ongoing debates around whether federal privacy legislation should include a private right of action, but it is important to note that many existing federal and state antidiscrimination statutes allow both individuals and government enforcers to sue companies for civil rights violations.[192] By the same token, individuals should have a legal right to sue data brokers that collect, process, or share personal data in a manner that leads to discriminatory outcomes. On the government side, any federal or local agency that contracts commercial data brokers should undergo robust racial equity and ethics training and improve community engagement on these topics.[193] Ultimately, though, government agencies need strict warrant requirements and public accountability over commercial data transactions to prevent abuse of power.

In addition, all companies (including data brokers) and government agencies that either develop or deploy automated inferences should regularly audit their processes and outcomes for disparate impact by gender, race, age, disability, or religion. These risk and impact assessments could evaluate the type and scope of personal information processed, high-level demographic information of affected individuals, measures to ensure privacy and data minimization, and completeness of training datasets, particularly around highly sensitive decisions related to law enforcement or public benefits. Moreover, private companies and government agencies should be required to report their findings to Congress and the FTC, which can use the data to advance research on data brokers and inform future recommendations to prevent algorithmic bias or privacy violations.

## LONGER-TERM ACTIONS: OPPORTUNITIES FOR FUTURE DIALOGUE AND RESEARCH

***Any new guardrails on U.S. government transactions with commercial data brokers must also safeguard individuals from the aggregation of "publicly available" information.***

Americans should have a legal right to privacy in their personal information, regardless of whether they download mobile apps, post on social media networks, drive cars in public areas, or shop online. Several recent surveys suggest shifts in public attitudes toward privacy, although the majority of Americans still expect companies to safeguard personal information. A 2022 Morning Consult poll, for example, found that 92 percent of baby boomers, compared to 70 percent of Generation Z, expects companies to adhere to minimum privacy standards.[194] As societal norms evolve in a digital era, it is possible for the conception of a "reasonable expectation of privacy" to change over time. Other traditional legal standards, such as the third-party doctrine, may lose relevance in a digital ecosystem powered by complex and nontransparent data transfers. Therefore, U.S. internet users need concrete privacy rights even in personal information that mobile apps and third-party data brokers exchange on the commercial market.

Because public information receives fewer constitutional protections, U.S. government agencies have stretched their interpretation of the term to the furthest possible limits. For instance, the DOD and the CIA consider publicly available data to be any information "available to the public by subscription or purchase"—a binary definition that even the January 2022 ODNI report acknowledges to be outdated.[195] Information should not be considered public if government authorities can access it only through commercial data brokers, which, in turn, must scrape it from millions of websites against their terms of service or purchase it from mobile apps. The ADPPA broadly exempts publicly available information from privacy requirements, including data from "a website or online service made available to all members of the public, for free or for a fee."[196] Yet, this language could potentially strip information from protections the moment it is posted online, even if it still poses privacy concerns. This definition might also include content that users do not voluntarily upload to the internet and are unable to retract, including images captured by surveillance cameras in public places, or facial recognition databases where a person appears in a photo background without their knowledge or consent.

While the long-term understanding of publicly available information will continue to evolve alongside society, Congress and government agencies can adhere to some basic principles more immediately. First, publicly available data should encompass only information that is reasonably accessible to the general population without paywalls, subscriptions, or advanced engineering knowledge. For example, if ICE needs to pay Barbaricum $2.1 to 5.5 million over five years to scrape online social media data, then that information should not be considered publicly available.[197] As one precedent, the Supreme Court held in *Department of Justice v. Reporters Committee for Freedom of the Press* (1989) that a person's rap sheet should not be considered public information, even if available through some channels, because it was difficult to access and therefore "practically obscure."[198]

Second, the definition of publicly available should be limited to content that individuals affirmatively choose to disseminate to a wide audience—and, unless it is a matter of significant public concern, they should be able to retract it at any time.[199] For instance, content that a politician uploads to their public Twitter account with millions of followers might be considered widespread dissemination, but the majority of Americans might not reasonably expect data miners to scrape personal photos intended for tight-knit circles like friends and family. Even in public areas, the geographic movements of most Americans are also not issues of public concern, and individuals often do not voluntarily choose to share them and cannot delete them under U.S. federal law. Public availability should not automatically void all privacy protections either; basic privacy protections should apply unless data are particularly newsworthy or serve a significant societal benefit.

***While data brokers need clear boundaries to prevent sales of sensitive personal information to adversarial individuals, companies, or governments, cross-border data flows are still vital to the United States and global economies.***

As surveillance technologies advance, several governments, including the European Union and China, have introduced measures that promote data localization or otherwise restrict cross-border data flows, citing national security or privacy grounds. But data localization alone cannot prevent privacy violations and sometimes enhances domestic government access to sensitive personal information. Moreover, overly broad restrictions on data flows can disrupt online communications and commerce, especially since almost all modern businesses operate websites or apps, conduct electronic global transactions, and otherwise depend on international data flows.

As the United States weighs various options to address national security risks posed by mobile apps like TikTok and data brokers, it is important to consider how blanket restrictions on cross-border data flows could create unintended long-term consequences. Data localization could prompt other countries to institute reciprocal limitations on the United States or weaken global negotiations on free flows of data in the future.[200] U.S. businesses have already experienced significant uncertainty after the CJEU's *Schrems I* and *Schrems II* decisions threatened to curtail transatlantic data flows. When France joined the United States in blocking TikTok on government-issued devices in March 2023, it also added U.S. apps like Twitter and Netflix to that list.[201] If even close political and economic allies like the European Union and United States cannot maintain trust in data flows, then further normalization of data localization could cause a breakdown of commerce and communications across the global economy. Moreover, even if forced data localization for TikTok or future non-U.S. mobile apps might slow foreign governments from accessing those specific databases, it could simultaneously streamline U.S. government access or potential misuse. Instead of data localization, the United States should promote free flows of information among allies along the lines of the Data Free Flow with Trust framework proposed under Japan's Group of Twenty (G20) leadership in 2019—a process that will require ongoing multilateral dialogues and understanding.

Some bills, like the Protecting Americans' Data from Foreign Surveillance Act of 2023, propose to use export control laws to prevent certain categories of personal information from being transferred to select foreign countries.[202] Tailored limitations like these could prevent all data brokers and private companies from selling exceptionally sensitive personal information abroad while maintaining overall cross-border data flows. In the end, though, comprehensive privacy measures are the best way to mitigate risk by reducing the amount of extraneous data available to foreign and domestic entities. All U.S. data brokers and private companies should follow certain fair information practice principles: minimizing data collection to specific purposes, deleting data after it is no longer necessary, allowing stronger transparency and oversight, and more.[203]

***Boundaries on data transfers must also balance values of free speech and expression.***

An individual's right to privacy can sometimes come into tension with First Amendment protections on free speech and communications, especially regarding dissemination of publicly available, aggregated, or de-identified information.[204] In *Sorrell v. IMS Health* (2011), the Supreme Court struck down a Vermont law that prevented pharmacies from selling prescription information to data brokers for marketing purposes, stating it could violate legal standards of "discrimination in expression" and commercial speech.[205] Hoan Ton-That, CEO of Clearview AI, has cited the First Amendment to defend the company's indiscriminate scraping of photos on public-facing websites.[206] Yet Clearview entered into a settlement agreement in *ACLU v. Clearview AI* (2022) to halt access to its facial recognition database to private businesses and individuals nationwide and to

temporarily pause sales to both public and private entities in Illinois under the state's Biometric Information Privacy Act.[207]

While the United States should avoid imposing overly restrictive limitations on information flows, stronger privacy protections can also promote values of free speech and expression.[208] China's surveillance laws demonstrate how forced censorship can also lead to self-censorship, as fear of government reprisal can prevent individuals from expressing themselves through public or private online channels. Closer to home, experts at the Brennan Center for Justice and Georgetown University's Institute for Technology Law and Policy warn that social media web scraping by U.S. federal and local police could have a chilling effect on constitutionally-protected environmental, reproductive rights, and racial equity activism.[209] In this manner, clear parameters on how U.S. government agencies collaborate with data brokers can safeguard individuals' right to speak openly, particularly for historically marginalized communities that have been disproportionately subjected to surveillance based on their race, religion, income, or location.

The First Amendment is strong but not absolute, as the government can impose tailored restrictions on speech to advance important interests like individual privacy.[210] However, sales of public, aggregated, and de-identified information are an underdiscussed aspect of federal privacy legislation. Additional congressional investigations and hearings may be necessary to gather civil society input on possible restrictions without raising undue censorship concerns. Furthermore, as Cameron F. Kerry and John B. Morris Jr. point out, legislative findings will be important to clarify congressional intent on this matter, which could help any forthcoming federal privacy bill withstand future constitutional challenges.[211]

***As data collection and algorithmic analysis advance, Congress should thoroughly reevaluate conventional constitutional and statutory limitations on both compelled and voluntary disclosure of data to U.S. government agencies as a long-term objective.***

In 2014, the White House published a report acknowledging

> the laws that govern protections afforded to our communications were written before email, the internet, and cloud computing came into wide use. Congress should amend ECPA to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world–including by removing archaic distinctions between email left unread or over a certain age.[212]

In addition to updating the ECPA to ensure consistent privacy standards across companies like data brokers, any forthcoming reauthorization of Title VII of the FISA Amendments Act should codify the EU-U.S. DPF into statute and consider modernized privacy safeguards.

The failure to update the ECPA and FISA for the big data era has resulted in archaic distinctions such as the type of device or length of time a message has been stored. The ECPA assigns privacy protections based on categories like metadata or communications content, but since data brokers often derive algorithmic inferences from multiple sources, it is difficult to neatly label modern datasets by type. Title I of the ECPA, commonly referred to as the Wiretap Act, requires the FBI to obtain a "super warrant" to intercept certain real-time communications, but Section 702 of FISA allows the FBI to query incidental communications concerning U.S. individuals without a warrant. The Stored Communications Act mandates a warrant to access electronic messages stored for less than 180 days but only a subpoena or court order for those stored longer than that time frame, even as the increasing affordability of data storage leads individuals and private companies to retain messages for longer periods.

While this report does not focus on compelled access requests under the ECPA and FISA, the rise of the data brokerage industry calls for a more holistic review of all forms of law enforcement access to private sector data. Congress can undertake this review by holding hearings and conducting investigations. The FTC reporting recommendations from subsection VIII (5) and (6) of this report would assist in this endeavor. Future discussions could also consider new statutory limitations on geofence or keyword warrants given their outsized potential to pose privacy or civil liberties risks to large numbers of individuals.

# Conclusion

To summarize, stronger privacy guardrails on the commercial data brokerage industry would present both short- and long-term benefits for the United States. First, these could enhance the nation's global reputation for data protection, which is essential to sustaining cross-border data flows and promoting economic stability for U.S. businesses. Even though many international dialogues like the EU-U.S. DPF continue to center around pre-Snowden compelled access to signals intelligence, instead of the rising prevalence of "voluntary" sales of personal information, clear boundaries on commercial data transactions could help build longer-term global confidence in both the U.S. public and private sectors.

Stricter privacy measures are also vital to national security since data brokers can accumulate detailed personal information and transmit it abroad in ways that could advantage foreign adversaries. However, privacy is not only an economic and national security imperative; it is also an important human and civil right. There are moral and ethical grounds to both directly regulate the data brokerage industry and also reduce U.S. government dependence on it, particularly in light of racial profiling patterns in law enforcement. Without explicit protocols to restrict their interactions with U.S. government agencies, commercial data brokers risk reinforcing the disproportionate oversurveillance of individuals by factors like race, religion, or income.

Lastly, there are geopolitical implications to consider. By limiting domestic government surveillance, the United States can demonstrate the importance of privacy values for the rest of the world. In turn, stronger U.S. privacy protections could provide a meaningful starting point for longer-term multilateral dialogues on limiting non-U.S. government transactions with data brokers. While the CCP should be held accountable for mass surveillance of its own citizens, particularly the Uyghur and Kazakh communities, the United States is in a weaker position to counteract China when it has made unjust arrests and deportations using personal

information acquired from millions of Americans without a warrant. As technology continues to advance, big data will become increasingly central to economics, national security, and human rights. Therefore, it is crucial to set strong precedents and smart policies for data brokers now in order to positively shape their interactions with government agencies for years to come.

# About the Author

**Caitlin Chin** is a fellow at the Center for Strategic and International Studies (CSIS), where she researches the impact of technology on geopolitics and society. Her current research interests include the relationships between data brokers and government agencies, the evolution of news in a digital era, and the role of technology platforms in countering online harmful content. Prior to joining CSIS, she previously worked as a research analyst at the Brookings Institution, where she primarily analyzed developments in U.S. federal and state data privacy legislation. At Brookings, Chin coauthored "Bridging the gaps: A path forward to federal privacy legislation" (with Cameron Kerry, John Morris Jr., and Nicol Turner Lee), which put forward a comprehensive framework for national commercial privacy standards in the United States. Her work has been published with CSIS, the Brookings Institution, Slate, Barron's, the *Georgetown Journal of International Affairs*, the *Georgetown Public Policy Review*, and the University of Pennsylvania's *Regulatory Review*. In addition, she has provided commentary for U.S. and international television, radio, and digital news outlets such as the *New York Times*, CNN, CBS News, and BBC News. She has a BA in government and Spanish from the University of Maryland and an MPP from Georgetown University's McCourt School of Public Policy. Her master's thesis, "Examining national privacy laws in the context of international trade," won a student paper award at the 48th Research Conference on Communications, Information, and Internet Policy (TPRC48) in 2020. She was also a recipient of Public Knowledge's 20/20 Visionaries award in 2021.

# Endnotes

1 Matt Spetalnick and Steve Holland, "Obama Defends Surveillance Effort as 'Trade-Off' for Security," Reuters, June 7, 2013, https://www.reuters.com/article/us-usa-security-records/obama-defends-surveillance-effort-as-trade-off-for-security-idUKBRE9560VA20130608.

2 Edward Snowden Compares Privacy to Freedom of Speech," University of Arizona, March 28, 2016, https://news.arizona.edu/story/edward-snowden-compares-privacy-freedom-speech; and Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, CT: Yale University Press, 2011), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2092&context=faculty_publications.

3 Brad Smith, "The Secret Gag Orders Must Stop," *Washington Post*, June 13, 2021, https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/.

4 Dell Cameron, "The US Is Openly Stockpiling Dirt on All Its Citizens," *Wired*, June 12, 2023, https://www.wired.com/story/odni-commercially-available-information-report/; and "Report to the Director of National Intelligence," Office of the Director of National Intelligence, Senior Advisory Group, Panel on Commercially Available Information, January 27, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.

5 "Remarks by National Security Advisor Jake Sullivan at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit," White House, July 13, 2021, https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit/.

6 David Ingram, "Biden Signs TikTok Ban for Government Devices, Setting Up a Chaotic 2023 for the App," NBC News, December 30, 2022, https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724.

7 U.S. Senate Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry:*

*Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Washington, DC: Office of Oversight and Investigations Majority Staff, December 2013), https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a.

8 "Information Requests Report," TikTok, December 2, 2021, https://www.tiktok.com/transparency/en-us/information-requests-2021-1/.

9 Caitlin Chin, "Digital Dragnets: Examining the Government's Access to Your Personal Information," CSIS, *Testimony*, July 19, 2022, https://www.csis.org/analysis/digital-dragnets-examining-governments-access-your-personal-data.

10 Caitlin Chin, "U.S. Digital Privacy Troubles Do Not Start or End with TikTok," CSIS, *Commentary*, October 6, 2022, https://www.csis.org/analysis/us-digital-privacy-troubles-do-not-start-or-end-tiktok.

11 John Podesta, "Findings of the Big Data and Privacy Working Group Review," White House, May 1, 2014, https://obamawhitehouse.archives.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.

12 FTC, *Data Brokers*: *A Call for Transparency and Accountability* (Washington, DC: FTC, May 2014), 11–12, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

13 FTC, *Data Brokers*, iv.

14 Ibid., vi.

15 Ibid., 1.

16 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.

17 Cal. Civ. Code § 1798.99.801, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.48.&part=4.&chapter=&article.

18 "Data Broker Registry," California Office of the Attorney General, https://oag.ca.gov/data-brokers.

19 American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152.

20 Boris Lubarsky, "Re-identification of 'Anonymized' Data," *Georgetown Law Technology Review* 202 (April 2017), https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

21 Adam Tanner, "Harvard Professor Re-identifies Anonymous Volunteers in DNA Study," *Forbes*, April 25, 2013, https://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/; and Latanya Sweeney, Akua Abu, and Julia Winn, "Identifying Participants in the Personal Genome Project by Name," Harvard University Data Privacy Lab, April 24, 2013, https://dataprivacylab.org/projects/pgp/1021-1.pdf.

22 *Testimony before the U.S. Senate Committee on Judiciary, Subcommittee on Privacy, Technology, and the Law: Hearing on Protecting Americans' Privacy Information from Hostile Foreign Powers,* 117th Cong. (2022) (statement of Susan Landau, Bridge Professor of Cyber Security and Policy, Fletcher School and School of Engineering, Department of Computer Science, Tufts University), https://www.judiciary.senate.gov/imo/media/doc/Testimony%20-%20Landau%20-%202022-09-14.pdf.

23 "Warren, Booker, Wyden Call on Mental Health Apps to Provide Answers on Data Privacy and Sharing Practices That May Put Patients' Data at Risk of Exploitation," Elizabeth Warren, June 23, 2022, https://

www.warren.senate.gov/oversight/letters/warren-booker-wyden-call-on-mental-health-apps-to-provide-answers-on-data-privacy-and-sharing-practices-that-may-put-patients-data-at-risk-of-exploitation.

24 Bennett Cyphers, "Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police," Electronic Frontier Foundation, August 31, 2022, https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police.

25 Caitlin Chin, "What Privacy in the United States Could Look Like Without *Roe v. Wade*," CSIS, *Critical Questions*, May 25, 2022, https://www.csis.org/analysis/what-privacy-united-states-could-look-without-roe-v-wade; and Jacob Kastrenakes, "Homeland Security Reportedly Bought Phone Location Data to Track People at the Border," The Verge, February 7, 2020, https://www.theverge.com/2020/2/7/21127795/dhs-buying-phone-location-data-marketing-companies-border-immigration.

26 FTC, *Data Brokers*.

27 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.

28 Lois Beckett, "Everything We Know about What Data Brokers Know about You," ProPublica, June 13, 2014, https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

29 Ibid.

30 Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals* (Durham, NC: Duke University, August 2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

31 Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data without Warrants, Memo Says," *New York Times*, January 22, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html; Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," Vice, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Bennett Cyphers, "How the Federal Government Buys Our Cell Phone Location Data," Electronic Frontier Foundation, June 13, 2022, https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data; and Shreya Tewari and Fikayo Walter-Johnson, "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data," ACLU, July 18, 2022, https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data.

32 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; and Will Knight, "Clearview AI Has New Tools to Identify You in Photos," *Wired*, October 4, 2021, https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.

33 "Social Media Surveillance by Homeland Security Investigations: A Threat to Immigrant Communities and Free Expression," Brennan Center for Justice, November 15, 2019, https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-homeland-security-investigations-threat; and *Visa Overstays: A Gap in the Nation's Border Security: Hearing before the Subcommittee on Border and Maritime Security of the Committee on Homeland Security, House of Representatives*, 115th Cong. (2017), https://www.govinfo.gov/content/pkg/CHRG-115hhrg27610/pdf/CHRG-115hhrg27610.pdf.

34 "Definitive Contract 70CMSW20C0000000," Center for Democracy and Technology, March 17, 2021, https://cdt.org/wp-content/uploads/2021/12/Definitive-Contract-70CMSW20C00000001-ICE-5-5-million-Barbaricum-LLC-2020-2025.pdf.

35 Conor Friedersdorf, "An Unprecedented Threat to Privacy," *The Atlantic*, January 27, 2016, https://www.

theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/; and Thomson Reuters, "Thomson Reuters Brings Vigilant License Plate Recognition Data to CLEAR Investigation Platform," Press Release, June 18, 2017, https://www.thomsonreuters.com/en/press-releases/2017/june/thomson-reuters-brings-vigilant-license-plate-recognition-data-to-clear-investigation-platform.html.

36 Cyphers, "Inside Fog Data Science."

37 Allen, "Health Insurers."

38 Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data: The Exchange of Our Most Sensitive Data and What It Means for Personal Privacy* (Durham, NC: Duke University, February 2023), https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-americans-mental-health-data/.

39 U.S. Senate Committee on Commerce, Science, and Transportation, *A Review*; and Aaron Taube, "How Marketers Use Big Data to Prey on the Poor," Business Insider, December 19, 2013, https://www.businessinsider.com/how-marketers-use-big-data-to-prey-on-the-poor-2013-12.

40 "Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers," FTC, February 18, 2016, https://www.ftc.gov/news-events/news/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive-personal-information-scammers; and "FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts," FTC, December 23, 2014, https://www.ftc.gov/news-events/news/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars-consumers-accounts.

41 Matt O'Brien and Frank Bajak, "Priest Outed via Grindr App Highlights Rampant Data Tracking," Associated Press, July 22, 2021, https://apnews.com/article/technology-europe-business-religion-data-privacy-97334ed1aca5bd363263c92f6de2caa2.

42 Esther Salas, "My Son Was Killed Because I'm a Federal Judge," *New York Times*, December 8, 2020, https://www.nytimes.com/2020/12/08/opinion/esther-salas-murder-federal-judges.html; and Justin Sherman, "The Open Data Market and Risks to National Security," Lawfare, February 3, 2022, https://www.lawfareblog.com/open-data-market-and-risks-national-security.

43 Spencer Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine," The Intercept, March 2, 2017, https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/.

44 Edward Ongweso Jr., "Palantir's CEO Finally Admits to Helping ICE Deport Undocumented Immigrants," VICE, January 24, 2020, https://www.vice.com/en/article/pkeg99/palantirs-ceo-finally-admits-to-helping-ice-deport-undocumented-immigrants.

45 Alfred Ng, "Data Brokers Raise Privacy Concerns—but Get Millions from the Federal Government," *Politico*, December 21, 2022, https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600.

46 Carey Shenkman et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers* (Center for Democracy and Technology, December 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

47 *Hearing on Promoting Competition, Growth, and Privacy Protection in the Technology Sector, before the US Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth*, 116th Cong. (2021) (statement of Stacey Gray, Senior Counsel, Future of Privacy Forum), https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Stacey%20Gray%20(Dec.%207,%202021)%20-%20Senate%20Finance%20Subcommittee%20on%20Fiscal%20Responsibility%20and%20Economic%20Growth.pdf; "Fraud

Prevention Toolkit," Centers for Medicare and Medicaid Services, https://www.cms.gov/Outreach-and-Education/Outreach/Partnerships/FraudPreventionToolkit; and Ng, "Data Brokers."

48 Drew Harwell, "ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations," *Washington Post*, February 26, 2021, https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/.

49 Sarah Lamdan, "The Quiet Invasion of 'Big Information,'" *Wired*, November 9, 2022, https://www.wired.com/story/big-information-relx-privacy-surveillance-data/.

50 "*Gonzalez v. ICE*," National Immigrant Justice Center, September 30, 2019, https://immigrantjustice.org/court_cases/gonzalez-v-ice; Sherman, "The Open Data Market"; and Gerardo Gonzalez, et al., v. Immigration and Customs Enforcement, et al., 416 F. Supp. 3d 995 (C.D. Cal. 2019), https://www.courthousenews.com/wp-content/uploads/2019/09/Gonzalez.v.ICE_.detainer.final_.order_.9.27.pdf.

51 Meghan Koushik, "Data Brokers Know a Lot about You, but What Do You Know about Them?" Brennan Center for Justice, October 31, 2014, https://www.brennancenter.org/our-work/analysis-opinion/data-brokers-know-lot-about-you-what-do-you-know-about-them.

52 Matt Stroud, "Heat Listed," The Verge, May 24, 2021, https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list.

53 Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: New York University Press, 2017), 131–35.

54 "Social Media Surveillance," Brennan Center for Justice.

55 *Hearing before the U.S. House Judiciary Committee*, 117th Cong. (2022) (statement of Rebecca Wexler, Co-Director, Berkeley Center for Law and Technology), https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-WexlerR-20220719.pdf.

56 Nicol Turner Lee and Caitlin Chin, "Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color," Brookings Institution, April 12, 2022, https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

57 Cox, "How the U.S. Military Buys"; and Joseph Cox, "More Muslim Apps Worked with X-Mode, Which Sold Data to Military Contractors," VICE, January 28, 2021, https://www.vice.com/en/article/epdkze/muslim-apps-location-data-military-xmode.

58 "FTC Sues Kochava for Selling Data That Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations," FTC, August 29, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

59 "Warren, Maloney, Wyden, DeSaulnier Probe Data Broker's Collection of Data on Black Lives Matter Demonstrators," Elizabeth Warren, August 4, 2020, https://www.warren.senate.gov/oversight/letters/warren-maloney-wyden-desaulnier-probe-data-brokers-collection-of-data-on-black-lives-matter-demonstrators; Max Rivlin-Nadler, "How ICE Uses Social Media to Surveil and Arrest Immigrants," The Intercept, December 22, 2019, https://theintercept.com/2019/12/22/ice-social-media-surveillance/; and Mary Pat Dwyer and José Guillermo Gutiérrez, "Documents Reveal LAPD Collected Millions of Tweets from Users Nationwide," Brennan Center for Justice, December 15, 2021, https://www.brennancenter.org/our-work/analysis-opinion/documents-reveal-lapd-collected-millions-tweets-users-nationwide.

60 Amanda Peacher, "Why Is the State of Oregon Conducting Intelligence Work?" Jefferson Public Radio, May 24, 2018, https://www.ijpr.org/2018-05-24/why-is-the-state-of-oregon-conducting-intelligence-work.

61 Rani Molla, "Law Enforcement Is Now Buying Cellphone Location Data from Marketers," Vox, February 7, 2020, https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration; and Tewari and Walter-Johnson, "New Records."

62 Zach Dorfman, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe," *Foreign Policy*, December 21, 2020, https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.

63 Cate Cadell, "China Harvests Masses of Data on Western Targets, Documents Show," *Washington Post*, December 31, 2021, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html.

64 Muyi Xiao and Paul Mozur, "A Digital Manhunt: How Chinese Police Track Critics on Twitter and Facebook," *New York Times*, December 31, 2022, https://www.nytimes.com/2021/12/31/technology/china-internet-police-twitter.html.

65 Stuart A. Thompson and Charlie Warzel, "How to Track President Trump," *New York Times*, December 20, 2019, https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html.

66 Shreya Tewari, "How to Navigate Mental Health Apps That May Share Your Data," ACLU, September 28, 2022, https://www.aclu.org/news/privacy-technology/how-to-navigate-mental-health-apps-that-may-share-your-data; and Justin Sherman, "Your Health Data Might Be for Sale," Slate, June 22, 2022, https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

67 Byron Tau, "The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots," *Wall Street Journal*, April 26, 2021, https://www.wsj.com/articles/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402; and Jessica Dawson and Brandon Pugh, "Ukraine Conflict Heightens US Military's Data Privacy Vulnerabilities," C4ISRNET, April 14, 2022, https://www.c4isrnet.com/opinion/2022/04/14/ukraine-conflict-heightens-us-militarys-data-privacy-vulnerabilities/.

68 Tau, "The Ease of Tracking."

69 Jeremy Hsu, "The Strava Heat Map and the End of Secrets," *Wired*, January 19, 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/; and Jeffrey Lewis, "Fitness-Tracker App Exposes Security Flaw at Taiwan's Missile Command Center," Daily Beast, January 28, 2018, www.thedailybeast.com/strava-fitness-tracker-app-exposes-taiwans-missile-command-center.

70 Sherman, "Data Brokers."

71 Nikhil Sonnad, "The Chinese Military Is Afraid Wearables Will Reveal Its Secrets," Quartz, May 11, 2015, https://qz.com/402353/the-chinese-military-is-afraid-wearables-will-reveal-its-secrets.

72 Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million through Facebook Alone," *New York Times*, October 30, 2017, https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html; and Scott Shane and Vindu Goel, "Fake Russian Facebook Accounts Bought $100,000 in Political Ads," *New York Times*, September 6, 2017, https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html.

73 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/; Donie O'Sullivan and Dylan Byers, "Exclusive: Fake Black Activist Accounts Linked to Russian Government," CNN, September 28, 2017, https://money.cnn.com/2017/09/28/media/blacktivist-russia-facebook-twitter/index.html; and Tim Mak, "Senate Report: Russians Used Social Media Mostly to Target Race in 2016," NPR, October 8, 2019, https://www.npr.org/2019/10/08/768319934/senate-report-russians-used-used-social-media-mostly-to-target-race-in-2016.

74 Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, S. Doc. 116-XX, vol. 2, at 83 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

75 Geoffrey A. Fowler, "How Politicians Target You: 3,000 Data Points on Every Voter, including Your Phone Number," *Washington Post*, October 27, 2020, https://www.washingtonpost.com/technology/2020/10/27/political-campaign-data-targeting/.

76 Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *New York Times*, March 17, 2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

77 Richard Behar, "Never Heard of Acxiom? Chances Are It's Heard of You. How a Little-Known Little Rock Company—the World's Largest Processor of Consumer Data—Found Itself at the Center of a Very Big National Security Debate," CNN Money, February 23, 2004, https://money.cnn.com/magazines/fortune/fortune_archive/2004/02/23/362182/index.htm.

78 Lesley Fair, "$575 Million Equifax Settlement Illustrates Security Basics for Your Business," FTC, July 22, 2019, https://www.ftc.gov/business-guidance/blog/2019/07/575-million-equifax-settlement-illustrates-security-basics-your-business.

79 Dymples Leong and Teo Yi-Ling, "Data Brokers: A Weak Link in National Security," *The Diplomat*, August 21, 2020, https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security/.

80 Steven J. Arango, "Data Brokers Are a Threat to National Security," U.S. Naval Institute, December 2022, https://www.usni.org/magazines/proceedings/2022/december/data-brokers-are-threat-national-security.

81 *Hearing on Identity Theft and Data Broker Services, before the Committee on Commerce, Science, and Transportation*, 109th Cong. (2005), https://www.govinfo.gov/content/pkg/CHRG-109shrg61787/html/CHRG-109shrg61787.htm.

82 *Testimony on Protecting Americans' Private Information from Hostile Foreign Powers, before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law*, 117th Cong. (2022) (statement of Adam I. Klein, Director, Robert Strauss Center on International Security and Law University of Texas at Austin), https://www.judiciary.senate.gov/imo/media/doc/Testimony%20-%20Klein%20-%202022-09-14.pdf.

83 Alan Rappeport, "U.S. Outlines Plans to Scrutinize Chinese and Other Foreign Investment," *New York Times*, September 17, 2019, https://www.nytimes.com/2019/09/17/us/politics/china-foreign-investment-cfius.html.

84 Justin Sherman, "GoodRx, Health Data Brokerage, and the Limits of HIPAA," Lawfare, March 6, 2023, https://www.lawfareblog.com/goodrx-health-data-brokerage-and-limits-hipaa.

85 Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2013), https://www.law.cornell.edu/uscode/text/20/1232g; and Jeffrey Selingo, "Colleges Use Predictive Data, Analytics to Find Students," *The Atlantic*, April 11, 2017, https://www.theatlantic.com/education/archive/2017/04/how-colleges-find-their-students/522516/.

86 Stacey Gray and Pollyanna Sanderson, *Policy Brief: Location Data under Existing Privacy Laws* (Washington, DC: Future of Privacy Forum, December 2020), https://fpf.org/wp-content/uploads/2020/12/FPF_Guide_Location_Data_v2.2.pdf.

87 The Utah Consumer Privacy Act does not offer the right to correction. See, for example, "State Laws Related to Digital Privacy," National Conference of State Legislatures, June 7, 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

88 Justin Sherman, "Examining State Bills on Data Brokers," Lawfare, May 31, 2022, https://www.lawfareblog.com/examining-state-bills-data-brokers.

89 Matthew M. K. Stein, "Nevada Expands Do-Not-Sell Right to Cover Data Brokers," Manatt, Phelps & Phillips, June 8, 2021, https://www.manatt.com/insights/newsletters/privacy-and-data-security/nevada-expands-do-not-sell-right-to-cover-data-bro.

90 "Dissenting Statement of Commissioner Maureen K. Ohlhausen in the Matter of Nomi Technologies, Inc.," FTC, August 28, 2015, https://www.ftc.gov/system/files/documents/public_statements/799571/150828nomitechmkostatement.pdf.

91 Sherman, "Data Brokers."

92 "FTC Sues Kochava."

93 FTC, "FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices," Press Release, August 11, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices; and "Statement of Chair Lina M. Khan Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking Commission File No. R111004," FTC, August 11, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20on%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

94 Federal Trade Commission v. Kochava Inc., No. 2:22-cv-00377-BLW (ID. Ct. 2023), https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/court-dismissal-ftc-suit-against-kochava-5-4-23.pdf.

95 Caitlin Chin and Marla Odell, "Highlights: Commissioners Discuss the Future of the FTC's Role in Privacy," Brookings Institution, November 5, 2019, https://www.brookings.edu/blog/techtank/2019/11/05/highlights-commissioners-discuss-the-future-of-the-ftcs-role-in-privacy/.

96 Elizabeth Goitein, "The Government Can't Seize Your Digital Data. Except by Buying It," *Washington Post*, April 26, 2021, https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.

97 Ron Wyden to Ajit Pai, Washington, DC, May 8, 2018, https://www.documentcloud.org/documents/4457320-Wyden-Securus-Location-Tracking-Letter-to-FCC.html; and Micah Singleton, "Verizon Will Stop Selling Real-Time Location Data to Third-Party Brokers," The Verge, June 19, 2018, https://www.theverge.com/2018/6/19/17478934/verizon-selling-real-time-location-data-third-party-securus-wyden.

98 Podesta, "Findings."

99 "Fourth Amendment," Cornell Law School, Legal Information Institute, https://www.law.cornell.edu/constitution/fourth_amendment; and Katz v. United States, 389 U.S. 347, 351-352 (1967), https://www.law.cornell.edu/supremecourt/text/389/347.

100 Caitlin Chin, "Highlights: Setting Guidelines for Facial Recognition and Law Enforcement," Brookings Institution, December 9, 2019, https://www.brookings.edu/blog/techtank/2019/12/09/highlights-setting-guidelines-for-facial-recognition-and-law-enforcement/.

101 Thomson Reuters, "Thomson Reuters Brings Vigilant License Plate Recognition Data to CLEAR Investigation Platform"; and Friedersdorf, "An Unprecedented Threat."

102 Friedersdorf, "An Unprecedented Threat."

103 Rivlin-Nadler, "How ICE Uses"; and "Social Media Surveillance," Brennan Center for Justice.

104 John Villasenor, "What You Need to Know about the Third-Party Doctrine," *The Atlantic*, December 30, 2013, https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/; United States v. Miller, 425 U.S. 435 (1976); and Smith v. Maryland, 442 U.S. 735 (1979).

105 Carpenter v. United States, 138 S.Ct. 2206 (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

106 "Clarification of Information Briefed during DIA's 1 December Briefing on CTD," DIA, January 15, 2021, https://www.wyden.senate.gov/imo/media/doc/011521%20CTD%20Discussion%20RFI%20Response_redaction.pdf.

107 Hamed Aleaziz and Caroline Haskins, "DHS Authorities Are Buying Moment-by-Moment Geolocation Cellphone Data to Track People," BuzzFeed News, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

108 "Report to the Director of National Intelligence," Office of the Director of National Intelligence, Senior Advisory Group, Panel on Commercially Available Information.

109 Shenkman et al., *Legal Loopholes*.

110 Orin S. Kerr, *Buying Data and the Fourth Amendment*, Aegis Series Paper No. 2109 (Stanford, CA: Hoover Institution, 2021, https://www.hoover.org/sites/default/files/research/docs/kerr_webreadypdf.pdf.

111 Orin Kerr, "The Fourth Amendment and Geofence Warrants: A Critical Look at United States v. Chatrie," Lawfare, March 12, 2022, https://www.lawfareblog.com/fourth-amendment-and-geofence-warrants-critical-look-united-states-v-chatrie; Jennifer Lynch, "Federal Court in Virginia Holds Geofence Warrant Violates Constitution," Electronic Frontier Foundation, March 10, 2022, https://www.eff.org/deeplinks/2022/03/federal-court-virginia-holds-geofence-warrant-violates-constitution; and United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2019), https://www.eff.org/files/2022/03/10/us_v_chatrie-opinion_on_suppression_motion.pdf.

112 Saraphin Dhanani, "The D.C. District Court Upholds the Government's Geofence Warrant Used to Identify Jan. 6 Rioters," Lawfare, March 10, 2023, https://www.lawfareblog.com/dc-district-court-upholds-governments-geofence-warrant-used-identify-jan-6-rioters.

113 "Declaration on Government Access to Personal Data Held by Private Sector Entities," OECD, December 13, 2022, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

114 Aaron Rieke et al., *Data Brokers in an Open Society* (London: Upturn and Open Society Foundations, November 2016), https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf; "Personal Data Brokers and Consumer Profiling: GDPR Rules and Compliance with Article 5(3) of Directive 2002/58/EC," European Parliament, October 1, 2019, https://www.europarl.europa.eu/doceo/document/E-8-2019-000054_EN.html; and David Lazarus, "Column: Shadowy Data Brokers Make the Most of Their Invisibility Cloak," *Los Angeles Times*, November 5, 2019, https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

115 "Our Complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad," Privacy International, November 8, 2018, https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad; Amit Katwala, "Forget Facebook, Mysterious Data Brokers Are Facing GDPR Trouble," *Wired*, August 11, 2018, https://www.wired.co.uk/article/gdpr-acxiom-experian-privacy-international-data-brokers; and Aliya Ram and Madhumita Murgia, "Data Brokers: Regulators Try to Rein in the 'Privacy Deathstars,'" *Financial Times*, January 7, 2019, https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.

116 Ram and Murgia, "Data Brokers."

117 "Norwegian DPA Imposes Fine against Grindr LLC," European Data Protection Board, December 21, 2021, https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-imposes-fine-against-grindr-llc_en.

118 Natasha Lomas, "Oracle's 'Surveillance Machine' Targeted in US Privacy Class Action," TechCrunch, August 22, 2022, https://techcrunch.com/2022/08/22/oracle-us-privacy-class-action/.

119 Frits Gerritzen et al., "Netherlands: One of the First Major Privacy Class Actions Dismissed by Court of Amsterdam," Allen & Overy, February 3, 2022, https://www.jdsupra.com/legalnews/netherlands-one-of-the-first-major-2996284/.

120 "Facial Recognition: 20 Million Euros Penalty against Clearview AI," CNIL, October 20, 2022, https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai; and Natasha Lomas, "France Fines Clearview AI Maximum Possible for GDPR Breaches," TechCrunch, October 20, 2022, https://techcrunch.com/2022/10/20/clearview-ai-fined-in-france/.

121 "Regulations: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016," Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/%20PDF/?uri=CELEX:32016R0679.

122 Piotr Foitzik, "Publicly Available Data under the GDPR: Main Considerations," IAPP, May 28, 2019, https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/.

123 Thorsten Wetzling, Lauren Sarkesian, and Charlotte Dietrich, "Solving the Transatlantic Data Dilemma," New America, December 2021, https://www.newamerica.org/oti/reports/solving-the-transatlantic-data-dilemma/chapter-3-government-access-to-personal-data-held-by-the-private-sector/.

124 Gennie Gebhart, "A Promising New GDPR Ruling against Targeted Ads," Electronic Frontier Foundation, December 9, 2022, https://www.eff.org/deeplinks/2022/12/promising-new-gdpr-ruling-against-targeted-ads.

125 Mark Scott and Vincent Manancourt, "Google and Data Brokers Accused of Illegally Collecting People's Data: Report," *Politico*, September 21, 2020, https://www.politico.eu/article/google-and-data-brokers-accused-of-illegally-collecting-data-report/.

126 Matt Burgess, "How GDPR Is Failing," *Wired*, May 23, 2022, https://www.wired.com/story/gdpr-2022; and "Lack of Resources Puts Enforcement of Individuals' Data Protection Rights at Risk," European Data Protection Board, September 13, 2022, https://edpb.europa.eu/news/news/2022/lack-resources-puts-enforcement-individuals-data-protection-rights-risk_en.

127 "DPC Publishes Statistical Report on Handling of Cross-Border Complaints under GDPR's One-Stop-Shop (OSS)," Data Protection Commission, March 15, 2022, https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-statistical-report-handling-cross-border-complaints-under-gdprs-one-stop-shop-oss.

128 Estelle Massé, *Three Years under the EU GDPR: An Implement Progress Report* (New York: Access Now, May 2021), https://www.accessnow.org/wp-content/uploads/2021/05/Three-Years-Under-GDPR-report.pdf; and Luca Bertuzzi, "10 Years After: The EU's 'Crunch Time' on GDPR Enforcement," International Association of Privacy Professionals, June 28, 2022, https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement/.

129 "Review Report 74 on Automated OSINT by the AIVD and the MIVD" [Toezichtsrapport 74 over Automated OSINT door de AIVD en de MIVD], Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten [Review Committee on the Intelligence and Security Services], 2022, https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-automated-osint; and Thorsten Wetzling and Charlotte Dietrich, *Disproportionate Use of Commercially and Publicly Available Data: Europe's Next Frontier for Intelligence Reform?* (Berlin:

Stiftung Neue Verantwortung, November 2022), 10, https://www.stiftung-nv.de/sites/default/files/snv_commercially_available_data.pdf.pdf.

130 Ibid., 23.

131 Ibid., 34.

132 "Charter of Fundamental Rights of the European Union (2012/C 326/02)," Official Journal of the European Union, October 26, 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT.

133 "European Convention on Human Rights – Article 8," European Union Agency for Fundamental Rights, http://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0.

134 Council of Europe, *Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (Strasbourg, France: Council of Europe, June 2018), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

135 Thorsten Wetzling and Charlotte Dietrich, *Report on the Need for a Guidance Note on Article 11 on the Modernised Convention 108* (Strasbourg, France: Council of Europe, June 11, 2021), https://rm.coe.int/t-pd-2021-6-draft-guidance-note-on-exceptionsunder-article-11-of-the-/1680a2d512.

136 European Parliament and Council of the European Union, Directive (EU) 2016/680 (April 27, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680.

137 Laura Drechsler, "The Achilles Heel of EU Data Protection in a Law Enforcement Context: International Transfers under Appropriate Safeguards in the Law Enforcement Directive," in *Cybercrime: New Threats, New Responses: Proceedings of the XVth International Conference on Internet, Law & Politics* (Barcelona: Huygens Editorial, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3664125.

138 "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (2021/2016[COD])," European Commission, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN; and European Council, "Artificial Intelligence Act: Council Calls for Promoting Safe AI That Respects Fundamental Rights," Press release, December 6, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/.

139 Zina Chatzidimitriadou, Josefine Sommer, and Eva von Mühlenen, "Proposal for EU Artificial Intelligence Act Passes Next Level—Where Do We Stand and What's Next?" Sidley Austin, December 12, 2022, https://www.sidley.com/en/insights/newsupdates/2022/12/proposal-for-eu-artificial-intelligence-act-passes-next-level.

140 Luca Bertuzzi, "AI Act: EU Parliament's Discussions Heat Up over Facial Recognition, Scope," Euractiv, October 6, 2022, https://www.euractiv.com/section/digital/news/ai-act-eu-parliaments-discussions-heat-up-over-facial-recognition-scope/.

141 Chin, "The EU-U.S. Data Privacy Framework."

142 Ibid.

143 "The European Union's General Data Protection Regulation," Canadian Trade Commissioner Service, https://www.tradecommissioner.gc.ca/guides/gdpr-eu-rgpd.aspx?lang=eng.

144 Philippa Lawson and Jeffrey Vicq, "On the Data Trail: How Detailed Information about You Gets into the Hands of Organizations with Whom You Have No Relationship," Canadian Internet Policy and Public Interest Clinic, April 2006, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2005-

2006/p_200506_02/; and Jane Bailey, "Systematic Government Access to Private-Sector Data in Canada," *International Data Privacy Law* 2, no. 4 (November 2012): 216, https://academic.oup.com/idpl/article/2/4/207/676859.

145 National Security and Intelligence Review Agency, *NSIRA 2019 Annual Report* (Ottawa: NSIRA, November 2020), https://www.nsira-ossnr.gc.ca/html/2018-2019/index-eng.html.

146 Bailey, "Systematic Government Access."

147 Lawson and Vicq, "On the Data Trail."

148 "Police Use of Facial Recognition Technology in Canada and the Way Forward," Office of the Privacy Commissioner of Canada, June 10, 2021, https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

149 "Data Brokers: A Look at the Canadian and American Landscape," Office of the Privacy Commissioner of Canada, September 2014, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/db_201409/; Lawson and Vicq, "On the Data Trail"; Colin McClelland, "Data Brokers Are Tracking You—and Selling the Info," *Financial Post,* August 27, 2021, https://financialpost.com/technology/data-brokers-are-tracking-you-and-selling-the-info; and Bryan Short, "Mapping the Data Broker Economy (Blog 2): The Pelmorex Corporation," Open Media, September 15, 2022, https://openmedia.org/article/item/the-pelmorex-corporation.

150 "Protecting Privacy in an Intrusive World," Office of the Privacy Commissioner of Canada, June 2006, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_review_060718/.

151 Paul Vieira, "Canada Follows U.S., Europe with TikTok Ban on Government Devices," *Wall Street Journal*, February 27, 2023, https://www.wsj.com/articles/canada-follows-u-s-europe-with-tiktok-ban-on-government-devices-2273b07f.

152 Clare Duffy, "TikTok Sues Montana over New Law Banning the App," CNN, May 23, 2023, https://www.cnn.com/2023/05/22/tech/tiktok-montana-lawsuit/index.html.

153 Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

154 "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," Stanford Cyber Policy Center, DigiChina, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

155 Matt Burgess, "Ignore China's New Data Privacy Law at Your Peril," *Wired*, November 5, 2021, https://www.wired.com/story/china-personal-data-law-pipl/; Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," *New York Times*, May 17, 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html; and Amy Mackinnon, "How Russia is Strong-Arming Apple," *Foreign Policy*, January 31, 2019, https://foreignpolicy.com/2019/01/31/how-russia-is-strong-arming-apple-data-security-icloud/.

156 Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times,* April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

157 Ibid.

158 Paul Mozur and Aaron Krolik, "Spying Tools Turn China into Surveillance State, with Powerful Police," *Forbes*, December 18, 2019, https://www.forbesindia.com/article/special/spying-tools-turn-china-into-

surveillance-state-with-powerful-police/56689/1.

159 Muyi Xiao, Paul Mozur, and Gray Beltran, "Buying Influence: How China Manipulates Facebook and Twitter," *New York Times*, December 20, 2021, https://www.nytimes.com/interactive/2021/12/20/technology/china-facebook-twitter-influence-manipulation.html; and Xiao and Mozur, "A Digital Manhunt."

160 Mozur and Krolik, "Spying Tools."

161 Jay Cline and Joseph Nocera, "10 Ways China's New Data Rules Will Change Your Business," PwC, https://www.pwc.com/us/en/tech-effect/cybersecurity/china-pipl-rules-impact.html; Bingna Guo et al., "China Personal Information Protection Law Will Become Effective Soon," White and Case, September 22, 2021, https://www.whitecase.com/insight-alert/china-personal-information-protection-law-will-become-effective-soon; and Samm Sacks, "New China Data Privacy Standard Looks More Far-Reaching Than GDPR," CSIS, *Critical Questions*, January 29, 2018, https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.

162 "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021," Stanford Cyber Policy Center, DigiChina, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

163 Julia Zhu, "The Personal Information Protection Law: China's Version of the GDPR?" *Columbia Journal of Transnational Law*, February 14, 2022, https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr.

164 Cameron F. Kerry et al., "Bridging the Gaps: A Path Forward to Federal Privacy Legislation," Brookings Institution, June 3, 2020, https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/.

165 California Consumer Privacy Act of 2018, [1798.100 - 1798.199.100], https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

166 Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1265.

167 Protecting Military Servicemembers' Data Act of 2022, S. 4281, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/4281.

168 Protecting Americans' Data from Foreign Surveillance Act of 2022, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/4495.

169 Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party (ANTI-SOCIAL CCP) Act, H.R. 1081 and S. 347, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/1081.

170 DATA Act, H.R. 1153, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/1153.

171 Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act, S. 686, 118th Cong. (2023), https://www.warner.senate.gov/public/index.cfm/2023/3/senators-introduce-bipartisan-bill-to-tackle-national-security-threats-from-foreign-tech.

172 "Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act," White House, March 7, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/07/statement-from-national-security-advisor-jake-sullivan-on-the-introduction-of-the-restrict-act/.

173 Wetzling and Dietrich, *Disproportionate Use*.

174 Cameron F. Kerry et al., "Bridging the Gaps: A Path Forward to Federal Privacy Legislation," Brookings Institution, June 3, 2020, https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/.

175 "FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers," FTC, December 1, 2010, https://www.ftc.gov/news-events/news/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers-businesses-policymakers; "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace," United States Government Accountability Office, September 2013, https://www.gao.gov/assets/gao-13-663.pdf; FTC, *Data Brokers*; Ron Wyden, "Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy," Press Release, November 1, 2018, https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy; and Data Broker Accountability and Transparency Act of 2020, H.R. 6675, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/6675.

176 "National Do Not Call Registry," FTC, https://www.donotcall.gov/.

177 Cameron F. Kerry and Caitlin Chin, "Hitting refresh on Privacy Policies: Recommendations for Notice and Transparency," Brookings Institution, January 6, 2020, https://www.brookings.edu/blog/techtank/2020/01/06/hitting-refresh-on-privacy-policies-recommendations-for-notice-and-transparency/.

178 Rebecca Pifer, "FTC Sues Data Broker Kochava for Selling Data That Could Track Clinic Visits," Healthcare Dive, August 30, 2022, https://www.healthcaredive.com/news/ftc-data-broker-kochava-lawsuit-abortion-tracking-location/630805/; Ryan Mac, Caroline Haskins, and Antonio Pequeño IV, "Police in At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here," Buzzfeed News, August 25, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

179 FTC, *Data Brokers*.

180 Ellen Nakashima and Sari Horwitz, "Newly Declassified Documents on Phone Records Program Released," *Washington Post*, July 31, 2013, https://www.washingtonpost.com/world/national-security/governments-secret-order-to-verizon-to-be-unveiled-at-senate-hearing/2013/07/31/233fdd3a-f9cf-11e2-a369-d1954abcb7e3_story.html.

181 "Report to the Director of National Intelligence," Office of the Director of National Intelligence, Senior Advisory Group, Panel on Commercially Available Information.

182 Nicol Turner Lee, "Where Would Racial Progress in Policing Be without Camera Phones?" Brookings Institution, June 5, 2020, https://www.brookings.edu/blog/fixgov/2020/06/05/where-would-racial-progress-in-policing-be-without-camera-phones/.

183 Government Surveillance Transparency Act of 2022, S. 3888, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/3888; and NDO Fairness Act, H.R. 7072, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/7072.

184 Andrea Vittorio, "Google, Microsoft Back Bill Limiting Gag Orders on Data Demands," Bloomberg Law, July 7, 2022, https://news.bloomberglaw.com/privacy-and-data-security/google-microsoft-back-bill-limiting-gag-orders-on-data-demands; "Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b)," U.S. Department of Justice, Office of the Deputy Attorney General, October 19, 2017, https://aboutblaw.com/3JW; and Greg Nojeim and Jessie Miller, "Congress Needs to Make Surveillance Gag Orders Fair and Rare," Center for Democracy and Technology, August 5, 2022, https://cdt.org/insights/congress-needs-to-make-surveillance-gag-orders-fair-and-rare/.

185 "Annual Statistical Transparency Report: Calendar Year 2021," Office of the Director of National Intelligence, April 28, 2022, https://www.dni.gov/index.php/newsroom/reports-publications/reports-

publications-2022/item/2291-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2021.

186 Caitlin Chin and Marla Odell, "Highlights: Commissioners Discuss the Future of the FTC's Role in Privacy," Brookings Institution, November 5, 2019, https://www.brookings.edu/blog/techtank/2019/11/05/highlights-commissioners-discuss-the-future-of-the-ftcs-role-in-privacy/.

187 Chris Jay Hoofnagle, Woodrow Hartzog, and Daniel J. Solove, "The FTC Can Rise to the Privacy Challenge, but Not without Help from Congress," Brookings Institution, August 8, 2019, https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/; "GDP (Current US$) - United Kingdom," World Bank, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=GB; and "GDP (Current US$) - United States," World Bank, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US.

188 "EPIC Comments: Agenda for PCLOB May 2022 Meeting on Domestic Terrorism," Electronic Privacy Information Center, April 25, 2022, https://epic.org/documents/epic-comments-agenda-for-pclob-may-2022-meeting-on-domestic-terrorism/?_thumbnail_id=23594.

189 "Reps. Eshoo and Rush, Sen. Wyden Demand Investigation of Federal Agencies Surveilling Black Lives Matter Protests," Congresswoman Anna G. Eshoo, October 15, 2022, https://eshoo.house.gov/media/press-releases/reps-eshoo-and-rush-sen-wyden-demand-investigation-federal-agencies-surveilling.

190 Caitlin Chin, "Assessing Employer Intent When AI Hiring Tools Are Biased," Brookings Institution, December 13, 2019, https://www.brookings.edu/research/assessing-employer-intent-when-ai-hiring-tools-are-biased/.

191 Cameron F. Kerry, "Federal Privacy Legislation Should Protect Civil Rights," Lawfare, June 26, 2020, https://www.lawfareblog.com/federal-privacy-legislation-should-protect-civil-rights; and Danielle Keats Citron, "The US Needs to Recognize Intimate Privacy as a Civil Right," *Wired*, October 5, 2022, https://www.wired.com/story/privacy-intimacy-civil-rights-danielle-citron/.

192 Paula Bruening, "How to End the Deadlock on the Private Right of Action," International Association of Privacy Professionals, January 20, 2022, https://iapp.org/news/a/how-to-end-the-deadlock-on-the-private-right-of-action/.

193 Nicol Turner Lee and Caitlin Chin, "Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color," Brookings Institution, April 12, 2022, https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

194 Jordan Marlatt, "Data Privacy Is Different for Gen Z," Morning Consult, November 9, 2022, https://morningconsult.com/2022/11/09/data-privacy-is-different-for-gen-z/; and "Is Online Privacy Over? Finding from the USC Annenberg Center for the Digital Future Show Millennials Embrace a New Online Reality," University of Southern California, April 22, 2013, https://annenberg.usc.edu/news/faculty/online-privacy-over-findings-usc-annenberg-center-digital-future-show-millennials.

195 Shenkman et al., Legal Loopholes; and "DoD Manual 5240.01: Procedures Governing the Conduct of DoD Intelligence Activities," U.S. Department of Defense, August 8, 2016, https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf; and "Report to the Director of National Intelligence," Office of the Director of National Intelligence, Senior Advisory Group, Panel on Commercially Available Information.

196 American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152.

197 "Definitive Contract 70CMSW20C0000000," Center for Democracy and Technology.

198 "Addressing Government Partnerships with Data Brokers," CSIS," November 7, 2022, https://www.csis.org/events/addressing-government-partnerships-data-brokers; "Out of Sight, Out of Bounds," Reporters Committee for Freedom of the Press, 2009, https://www.rcfp.org/journals/the-news-media-and-the-law-spring-2009/out-sight-out-bounds/.

199 Dan Bischof, "Public Concern Outweighs Privacy," Reporters Committee for Freedom of the Press, 2001, https://www.rcfp.org/journals/the-news-media-and-the-law-summer-2001/public-concern-outweighs-pr/.

200 *Hearing on Promoting Competition, Growth, and Privacy Protection in the Technology Sector, before the US Senate Finance Subcomm. on Fiscal Responsibility and Economic Growth*, 116th Cong. (2021) (statement of Samm Sacks, Senior Fellow at Yale Law School's Paul Tsai China Center and Cybersecurity Policy Fellow at New America), https://www.finance.senate.gov/imo/media/doc/Samm%20Sacks%20Testimony%20-%20Senate%20Finance%20-%20December%207%202021.pdf.

201 "France Bans TikTok, Twitter from Government Staff Phones," Associated Press, March 24, 2023, https://apnews.com/article/tiktok-france-ban-cybersecurity-china-4c48564fbfe7b86bf44c30969902c293.

202 Protecting Americans' Data from Foreign Surveillance Act of 2022, S. 4495, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/4495.

203 "Records, Computers, and the Rights of Citizens," U.S. Department of Health and Human Services, June 30, 1973, https://aspe.hhs.gov/reports/records-computers-rights-citizens.

204 Bischof, "Public Concern"; and Robert C. Post and Jennifer E. Rothman, "The First Amendment and the Right(s) of Publicity," *Yale Law Journal* 130, no. 1 (October 2020): 86–172, https://www.yalelawjournal.org/article/the-first-amendment-and-the-rights-of-publicity.

205 Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011), https://www.supremecourt.gov/opinions/10pdf/10-779.pdf.

206 Hill, "The Secretive Company."

207 "In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law," ACLU, May 9, 2022, https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.

208 Margot E. Kaminski and Scott Skinner-Thompson, "Free Speech Isn't a Free Pass for Privacy Violations," Slate, March 9, 2020, https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html.

209 Gabriella Sanchez and Rachel Levinson-Waldman, "Police Social Media Monitoring Chills Activism," Brennan Center for Justice, November 18, 2022, https://www.brennancenter.org/our-work/analysis-opinion/police-social-media-monitoring-chills-activism; Sam Biddle, "U.S. Marshals spied on abortion protesters using Dataminr," The Intercept, May 15, 2023, https://theintercept.com/2023/05/15/abortion-surveillance-dataminr/.

210 Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional* (Oxford: Oxford University Press, 2014), https://law.yale.edu/sites/default/files/area/center/isp/documents/neil_richards_-_why_data_privacy_law_is_mostly_constitutional.pdf; and Kaminski and Skinner-Thompson, "Free Speech."

211 Cameron F. Kerry and John B. Morris Jr., "Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation," Brookings Institution, December 8, 2020, https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/.

212 "Big Data: Seizing Opportunities, Preserving Values," Executive Office of the President, May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

**COVER PHOTO** CARLOS LOPEZ-BARILLAS/LIAISON/GETTY IMAGES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**