BRENNAN CENTER FOR JUSTICE

The Honorable Rohit Chopra
Director, Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Dear Director Chopra:

The Brennan Center for Justice applauds the CFPB's initiation of a rulemaking process under the Fair Credit Reporting Act to protect the public against existing and potential harms created by the improper collection, aggregation, and sale of sensitive consumer information by the data broker industry.[1] We have previously raised concerns about the privacy, civil rights, and civil liberties threats that the under-regulated commercial data broker ecosystem imposes on consumers and called for stronger legal protections against those threats.[2] The purpose of this letter is to highlight the equally troubling risks that data brokers pose to national security.

Just as consumers' individual privacy interests are threatened by the unfettered harvesting, aggregation, analysis, and sale of personal data by commercial entities that

[1] Consumer Financial Protection Bureau, "Protecting the Public From Data Brokers in the Surveillance Industry," August 15, 2023, https://files.consumerfinance.gov/f/documents/cfpb-data-broker-rulemaking-faq_2023-08.pdf.

[2] For examples of the Brennan Center's advocacy regarding data brokers, see Emile Ayoub, "The Intelligence Community's Policy on Commercially Available Data Falls Short," Brennan Center for Justice, September 12, 2024, https://www.brennancenter.org/our-work/analysis-opinion/intelligence-communitys-policy-commercially-available-data-falls-short; Emile Ayoub and Elizabeth Goitein, "Closing the Data Broker Loophole," Brennan Center for Justice, February 13, 2024, https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole; Brennan Center for Justice, "Comments to the Federal Trade Commission re: Commercial Surveillance ANPR, R111004," November 21, 2022, https://www.rightsanddissent.org/wp-content/uploads/2022/12/FTC-comments-2022-Brennan-Center-et-al.pdf; *Digital Dragnets: Examining the Government's Access to Your Personal Data*, 117th Cong. (2022) (written testimony of Elizabeth Goitein, senior director of the Liberty and National Security program, Brennan Center for Justice), https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-GoiteinE-20220719.pdf; Elizabeth Goitein, "The Government Can't Seize Your Digital Data. Except by Buying It.," Brennan Center for Justice, April 28, 2021, https://www.brennancenter.org/our-work/analysis-opinion/government-cant-seize-your-digital-data-except-buying-it.

make up the data broker industry, so too are our collective security interests. As members of the President's Review Group on Intelligence and Communications Technologies explained in their 2013 report, privacy is an important form of security, and protecting it is essential to maintaining a free and democratic society.[3]

I am a fellow with the Brennan Center's Liberty and National Security program. I previously served for sixteen years as a special agent of the Federal Bureau of Investigation (1988-2004), the last twelve of which involved undercover operations in a variety of criminal cases, including domestic terrorism investigations. My undercover experience sensitized me to the difficulty of protecting one's identity data in an environment in which hostile actors have relatively easy access to the digital trails created by our increasing reliance on electronic technologies. As the scale of data surveillance by private companies has expanded, and data analytics have improved, the threats a poorly regulated data broker industry poses to law enforcement and intelligence operations and personnel—and the overall security of the American people—have become clearer.

Until recently, U.S. law enforcement and intelligence agencies operating in the post-9/11 environment rarely recognized or acknowledged these risks in public debates about data privacy, and instead prioritized the expansion of their own unfettered access to this data. Fortunately, this attitude is beginning to change as the risks have been increasingly realized.

The data broker industry threatens national security in at least three significant ways.

Malicious actors' access to sensitive data

First, consumer data about millions of Americans is a valuable commodity and any entity that collects and possess such data becomes a target for hostile actors, which puts all the individuals whose information is included in their databases at risk. The companies that harvest, aggregate, analyze, and sell data culled from ubiquitous commercial digital

[3] White House, Review Group on Intelligence and Communications Technologies, *Liberty and National Security in a Changing World*, December 12, 2013, 12, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

surveillance operations are lightly regulated, if at all. The information traded in these markets can reveal intimate details of Americans' lives, including their financial activities, addresses, occupations, health status, web browsing activity, cell phone location, political beliefs, associations, friends, and families. For decades, foreign governments have incurred significant expense to hire and train intelligence agents and analysts and deploy them abroad at great risk to obtain information about Americans that could provide just a fraction of the insights that can now be culled from purchased data at a much lower cost.[4] Just as the consumer information that the data broker industry sells is used by advertisers to find amenable audiences for ad campaigns, it can be used by foreign intelligence services to identify and target Americans who might be swayed by influence operations, confused by disinformation campaigns, susceptible to blackmail, or desperate for cash and vulnerable to recruitment.

Foreign intelligence agencies have reportedly used cyber-attacks to breach even well-resourced entities that employ sophisticated data protection protocols to protect the sensitive consumer data that they store, such as U.S. telecommunications companies like AT&T, Verizon, and Lumens,[5] credit reporting companies like Equifax,[6] and internet service providers like Yahoo.[7] Data brokers are much easier targets for these sophisticated hacking operations, which means they are vulnerable to relatively less capable criminal hacking groups as well. A criminal organization's 2023 hack of a relatively small Florida data broker called National Public Data exposed information that included 270 million Social Security numbers, as well as dates of birth, addresses, and

[4] Steven Arango, "Data Brokers: A Benefit or Peril to U.S. National Security?," *Ohio State Technology Law Journal* 20, no. 1 (June 2023): 119, https://kb.osu.edu/server/api/core/bitstreams/a9c18c3c-3b00-4918-9e90-6e2d538c9e54/content.

[5] Katrina Manson, "NSA Investigating Potential Chinese Hacking of American Telecom Firms," *Portland Press Herald*, October 7, 2024, https://www.pressherald.com/2024/10/07/nsa-investigating-if-chinese-hackers-breached-u-s-telecom-firms/.

[6] Federal Bureau of Investigation, "Chinese Military Hackers Charged in Equifax Breach," February 10, 2020, https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020.

[7] Eric Tucker, "Russian Agents, Hackers Charged in Massive Yahoo Breach," Associated Press, March 15, 2017, https://apnews.com/article/c78cb2fdff194169951dd768bb1d3dfd.

telephone numbers for up to 300 million people.[8] The lost data also reportedly included Drug Enforcement Administration licensing records for individuals authorized to write drug prescriptions, data identifying concealed weapons permit holders, marriage, divorce, and bankruptcy records. National Public Data filed for bankruptcy in the aftermath of the breach, leaving hundreds of million people with little recourse to mitigate their financial damages and recover the increased security expenses they will incur as a result of the breach.

It should also be noted that an analysis of the data exposed in the National Public Data hack performed by the media outlet TechCrunch found that a significant amount of information was inaccurate. TechCrunch attributed these inaccuracies to the nature of information collected and exchanged in data broker markets. The lack of regulations requiring data brokers to provide consumers with access to their personal data and the ability to correct or delete errors before the data is sold lowers data quality in the entire ecosystem. It also makes it easier for malicious actors within the data broker ecosphere to insert inaccurate information into the ecosystem that can harm particular individuals and breed public distrust of credit reporting systems, increasing costs across the board. A 2016 IMB study estimated that the poor data quality in the ecosystem costs the U.S. economy $3.1 trillion each year.[9]

Unlawful access to consumer data by corrupt insiders, criminal hackers, and foreign intelligence agencies that puts millions of Americans' financial and personal security at risk also creates a measurable impact on the U.S economy. In 2018, the Council of Economic Advisors estimated that malicious cyber activities cost the U.S. economy

[8] Zack Whittaker, "National Public Data, the Hacked Data Broker That Lost Millions of Social Security Numbers and More, Fles for Bankruptcy," *TechCrunch*, October 14, 2024, https://techcrunch.com/2024/10/14/national-public-data-the-hacked-data-broker-that-lost-millions-of-social-security-numbers-and-more-files-for-bankruptcy/.

[9] Manu Bansal, "Flying Blind: How Bad Data Undermines Business," *Forbes*, October 14, 2021, https://www.forbes.com/councils/forbestechcouncil/2021/10/14/flying-blind-how-bad-data-undermines-business/.

between $57 and $109 billion in 2016 alone.[10] In addition to the economic costs of unlawful data breaches, the volume and scope of Americans' personal data that is at risk in largely unregulated data markets creates an enormous and persistent national security vulnerability.

In fact, foreign intelligence services don't have to deploy cyber-attacks or risky intelligence operations to obtain Americans' consumer information from data brokers. They can simply purchase it on the open market, either directly through government-controlled companies or indirectly through witting or unwitting cut-outs. With access to the types of personal data exposed in the National Public Data breach, a foreign intelligence service could steal Americans' identities for use by their own agents, identify individuals for recruitment, fuel political or personal conflicts, and wreak financial havoc on targeted individuals. The Chinese government has reportedly issued contracts to create a vast social media data mining and surveillance network targeting U.S. and European social media accounts such as Twitter and Facebook, in order to censor criticism and promote pro-China propaganda.[11]

Risk to military, intelligence, and law enforcement officials

The second way the data broker industry harms national security is the direct threat it poses to federal, state, and local government employees, facilities, and operations. Hostile foreign entities target U.S. government employees to exploit their access to sensitive officials, facilities, equipment, documents, and data, as well as for their ability to influence official policies and obtain government resources.[12] Employees of government agencies are also consumers, and their personal data is open for collection and available for sale along with everyone else's. Data brokers often categorize the data they offer by

[10] White House, Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, February 2018, https://nsarchive.gwu.edu/sites/default/files/documents/5626430/Council-of-Economic-Advisors-The-Cost-of.pdf.

[11] 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.

[12] Arango, "Data Brokers," 119-122.

occupations and locations, making it easier for hostile actors to identify government employees working in sensitive fields, such as defense, law enforcement, and intelligence.

A recent study by Justin Sherman and his colleagues at Duke University's Sanford School of Public Policy underscored that many data brokers advertised data collections by specific categories, which included groupings of active military personnel and U.S. government employees, their family members, and close associates.[13] The data brokers marketed data collections that included criminal records, demographic data, income, credit card spending, student loans, location data, political affiliations, and even personality surveys.[14] The Duke researchers mimicked a foreign company by using a *.asia* domain and email with a Singaporean IP address to inquire about obtaining information regarding U.S. military personnel from U.S.-based data brokers. The researchers successfully purchased sensitive personal information including names, home addresses, emails, phone numbers, specific branch of service, health condition data, demographic information, gender, age, financial data, credit rating, and political affiliation for thousands of active-duty military members, their families, and friends.[15] The security threat posed by allowing foreign entities or other hostile actors access to this type of data is difficult to overstate.

By the nature of their work, law enforcement and intelligence officials, prosecutors, and judges, who are regularly exposed to criminals, terrorists, and hostile foreign government agents, are at increased risk of being targeted with violent attacks, harassment, doxing, blackmail campaigns, and recruitment operations. In 2019, New York Times journalists obtained anonymized cellphone location data from a company that collected it from

[13] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals,* Duke Sanford School of Public Policy, 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.

[14] Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*.

[15] Justin Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel*, Duke Sanford School of Public Policy, November 2023, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf.

tracking software in smartphone apps detailing the movements of more than 12 million Americans.[16] Using other publicly available records, the journalists were able to de-anonymize the data and identify and track U.S. Secret Service agents serving on President Trump's detail, as well as others working in national security.[17] The location data could be used to identify individuals' identities by tracking where they went home at night, and their employers by noting the cell phones' presence in courthouses, CIA parking lots, FBI, or Secret Service offices during work hours.

The trade in identity data puts law enforcement and intelligence officials who are operating in an undercover capacity at additional risk. The industry imperils the lives of undercover agents, and aids efforts to compromise law enforcement and intelligence operations at home and abroad. Former U.S. intelligence officials reported that China has already exploited the bulk data collections it obtained through "both legal and illegal means" to successfully expose U.S. intelligence assets.[18] Russians, likewise, are suspected of using payroll records to distinguish between State Department staff and intelligence officers operating under official cover at U.S. embassies.[19] While U.S. law enforcement and intelligence agencies have developed sophisticated methods to establish and protect alias identities, often at great expense, those efforts can be defeated with the smallest inconsistencies in the data, or an error in tradecraft. As one former intelligence official told Yahoo! News, "good backstopping can be defeated with a Google search."[20]

---

[16] Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[17] 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.

[18] 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/.

[19] Dorfman, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe."

[20] Jenna McLaughlin and Zach Dorfman, "'Shattered': Inside the Secret Battle to Save America's Undercover Spies in the Digital Age," Yahoo News, December 30, 2019,

The more data that is available in the data broker ecosystem and the wider its availability, the greater risk of compromise.

The advent of artificial intelligence increases the national security risks posed by an unregulated data market. For one thing, artificial intelligence will lead to improved data analysis tools, allowing hostile actors to exploit more effectively the wide variety of information available for sale in the data broker ecosystem to pierce undercover aliases and link them to an agent's true identity notwithstanding improved backstopping techniques. More broadly, artificial intelligence will likely fuel a wide range of new (and, to some degree, unpredictable) security threats, from producing undetectable malware and deepfakes, to facilitating cyber-espionage and kinetic attacks.[21] Since artificial intelligence requires big data sets to train and improve, stronger limits on data collection and transfers is an essential part of a mitigation strategy.[22]

U.S. government purchases that undermine security

The third way the data broker industry threatens national security is by enabling federal, state, and local government agencies in the United States to circumvent legal restrictions designed to protect Americans' sensitive personal information. These restrictions generally require government agencies to make some showing of need before acquiring personal data. Data brokers, which often fall through the cracks of outdated legal protections, provide a workaround that allows agencies to collect and store massive amounts of sensitive data with no demonstrated need.

---

https://www.yahoo.com/news/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html.

[21] Nate Lavoy, "Addressing the National Security Risks of Bulk Data in the Age of AI," RAND Corporation, August 23, 2024, https://www.rand.org/pubs/commentary/2024/08/addressing-the-national-security-risks-of-bulk-data.html.

[22] See Heidy Khlaaf et al., "Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting," arXiv (October 18, 2024), https://doi.org/10.48550/arXiv.2410.14831.

In addition to infringing on civil liberties,[23] unfettered access to Americans' data by government agencies poses a security risk. U.S. government databases, including those controlled by defense, intelligence, and law enforcement agencies, have not been immune from cyber-espionage, hackers, and leaks that have compromised operations and exposed the private information of Americans that has been collected at their expense.[24] The government's collection and retention of sensitive data of persons that are not reasonably suspected of presenting a criminal or national security threat creates unnecessary security vulnerabilities that must be weighed against the purported benefits they might provide.

To its credit, the U.S. intelligence community has recently acknowledged that its acquisition, retention, and use of commercially available information creates novel risks to the privacy and civil liberties of the American people.[25] In 2022, the Office of the Director of National Intelligence Senior Advisory Panel on Commercially Available Information noted that the intelligence community "currently acquires a significant amount of CAI for mission-related purposes, including in some cases social media data [redacted]and many other types of information."[26] The panel noted that the government's

---

[23] See Ayoub and Goitein, "Closing the Data Broker Loophole."

[24] See, e.g., Intercept, "BlueLeaks," accessed October 25, 2024, https://theintercept.com/collections/blueleaks/; Shane Harris and Dan Lamothe, "Intelligence Leak Exposes U.S. Spying on Adversaries and Allies," *Washington Post*, April 8, 2023, https://www.washingtonpost.com/national-security/2023/04/08/intelligence-leak-documents-ukraine-pentagon/; Julian E. Barnes and Adam Goldman, "Captured, Killed or Compromised: C.I.A. Admits to Losing Dozens of Informants," *New York Times*, October 5, 2021, https://www.nytimes.com/2021/10/05/us/politics/cia-informants-killed-captured.html.

[25] Office of the Director of National Intelligence, "Statement on the Intelligence Community's Policy Framework for Commercially Available Information," May 8, 2024, https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Statement-May2024.pdf.

[26] Office of the Director of National Intelligence, Senior Advisory Group, *Panel on Commercially Available Information*, January 27, 2022, 1, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.

purchase and retention of commercially available data creates risk to the privacy, civil liberties, and safety of the American people. It found that this data,

> "…can be misused to pry into private lives, ruin reputations, and cause emotional distress and threaten the safety of individuals. Even subject to appropriate controls, CAI can increase the power of the government's ability to peer into private lives to levels that may exceed our constitutional traditions or other social expectations. Mission creep can subject CAI collected for one purpose to other purposes that might raise risks beyond those originally calculated."[27]

In response to the panel's report, the ODNI issued a policy framework to establish uniform standards to govern how the 18 intelligence community agencies access, process, and collect commercially available information, and enhancing privacy and civil liberties protections.[28] The framework is a step forward in that it recognizes the need for greater privacy protections over this data, and may provide greater transparency regarding the government's acquisition of Americans' sensitive information. But it is insufficient in that it does not prohibit the intelligence agencies from purchasing data that would otherwise require a warrant, court order, or subpoena to obtain.[29]

Remedies

State and federal legislators have recognized the heightened risk to law enforcement officials and have begun taking steps to address them. A 2020 assassination attempt of U.S. District Court judge Esther Salas at her home in New Jersey, which resulted in the murder of her son, Daniel Anderl, raised concerns about the ease in which hostile actors can find the home addresses of government employees working in the criminal justice system. The New Jersey legislature passed a law, known as Daniel's Law, which allows current and former judicial officers, law enforcement officials, prosecutors, and their

[27] Senior Advisory Group, 11.

[28] Office of the Director of National Intelligence, "Statement on the Intelligence Community's Policy Framework for Commercially Available Information."

[29] Ayoub, "The Intelligence Community's Policy on Commercially Available Data Falls Short."

families to sue companies that publish their addresses or phone numbers on the Internet if they fail to respond to a take-down request in a timely manner.[30] Pennsylvania and the U.S. Congress have passed similar legislation to protect judges and judicial officers.[31] It remains to be seen whether these laws will prove effective in removing sensitive data from circulation through the data broker industry. In pending litigation, New Jersey police officers have filed 140 complaints against data brokers that failed to remove their addresses as the law required.[32] In any event, these laws will only scratch the surface of the national security issues discussed here.

In addition to the laws that have been enacted, there are bills that have been introduced in the U.S. Congress to address different aspects of the data broker problem. For instance, the House of Representatives this year passed the Fourth Amendment Is Not For Sale Act, which would prohibit intelligence and law enforcement agencies from purchasing communications-related information, location data, and illegitimately acquired information. The legislation has yet to move forward in the Senate, however, and it does not address sales to private entities. The American Privacy Rights Act, by contrast, would place significant restrictions on the collection, processing, and transfer of Americans'

[30] Alberto Luperon, New Jersey Passes 'Daniel's Law' After Misogynist Attorney Killed the Son of a Federal Judge, *Law & Crime*, November 23, 2020, https://lawandcrime.com/high-profile/new-jersey-passes-daniels-law-after-misogynist-attorney-killed-the-son-of-a-federal-judge/.

[31] Sandra Jones, "Shapiro Signs Bill Aimed at Protecting Federal Judges," WHYY, October 17, 2024, https://www.wesa.fm/politics-government/2024-10-17/pennsylvania-federal-judges-protection-legislation; United States Courts, "Congress Passes the Daniel Anderl Judicial Security and Privacy Act," December 16, 2022, https://www.uscourts.gov/news/2022/12/16/congress-passes-daniel-anderl-judicial-security-and-privacy-act.

[32] Tonya Riley, "Cops Battle Data Brokers for Privacy in Constitutional Clash," Bloomberg Law, September 30, 2024, https://news.bloomberglaw.com/privacy-and-data-security/cops-battle-data-brokers-for-privacy-in-constitutional-clash; see also KrebsonSecurity, "The Global Surveillance Free-for-All in Mobile Ad Data," October 23, 2024, https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data/.

data by companies, but it includes broad carveouts for access by law enforcement, and it faces political hurdles that will take time to overcome.[33]

A comprehensive solution to the data broker problem and the national security concerns it presents will require legislation. In the meantime, however, there are steps that agencies like the CFPB can and should take. Congress passed the Fair Credit Reporting Act (FCRA) to regulate the trade in consumer data and ensure it is used only for authorized purposes; the "data broker loophole" is undermining that intent. This squarely implicates the jurisdiction and responsibilities of the CFPB.

The Brennan Center supports the CFPB's efforts to require data brokers to comply with FCRA. These improvements include clarifying that personally identifying data in "credit header information" is a consumer report, and restricting data brokers' use and sharing of consumer data to permissible purposes, as defined in the statute. Applying FCRA requirements to data brokers would further protect consumers by allowing them to know what data the companies hold about them, and correct inaccuracies. These are important steps to improve the security of Americans' data, and thereby improve our national security as well.

Sincerely,

Michael German
Fellow, Liberty & National Security
Brennan Center for Justice at NYU School of Law

[33] Emile Ayoub, "Congress Must Act on Data Privacy," Brennan Center for Justice, May 28, 2024, https://www.brennancenter.org/our-work/analysis-opinion/congress-must-act-data-privacy; see also Ayoub and Goitein, "Closing the Data Broker Loophole."