CENTER FOR DEMOCRACY & TECHNOLOGY

July 15, 2023

To: Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Request for Information Regarding Data Brokers, Docket No. CFPB-2023-0020

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the Consumer Financial Protection Bureau's (CFPB) request for information (RFI) regarding data brokers.[1] CDT is a nonprofit 501(c)(3) organization that advocates to advance civil rights and civil liberties in the digital age. CDT's work includes protecting against privacy and data-related harms and exploitative and discriminatory uses of data.

The RFI expresses the CFPB's interest in data brokers whose business models involve selling consumer data, the harms to consumers that can result, and how the Fair Credit Reporting Act (FCRA) can be used to mitigate those harms. To help inform the CFPB's efforts, Part I of our comments describes data brokers'[2] practices around sourcing and selling or otherwise sharing consumer data, including financial data, worker data, health-related data, and location data. Part II of our comments addresses why certain measures ostensibly intended to protect consumer privacy in connection with data brokers' practices fall short. And Part III describes how the CFPB should build on its efforts to clarify the application of the FCRA to data brokers to minimize data sharing.

I. Data brokers obtain and share various types of data in ways that harm people.

The expansive data broker industry is built on clustering numerous types of personal data from a variety of sources and selling or otherwise providing that data to third parties. As the industry has grown, so has the severity of privacy- and data-related harms to consumers. For example,

[1] Consumer Financial Protection Bureau, *Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information*, Mar. 21, 2023, https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection.

[2] The RFI states that "data brokers" is "an umbrella term to describe firms that collect, aggregate, sell, resell, license, or otherwise share consumers' personal information with other parties." The RFI further explains that the term includes companies that share data from consumers with whom they interact directly as well as third parties that do not have a direct relationship with the consumers whose data they share. These comments address both of these categories of data brokers.

security researchers have uncovered poor security practices by multiple data brokers that have each exposed anywhere from tens of millions to over a billion people's information.[3] Data brokers also intentionally share people's data with entities that exploit it for a range of purposes, from marketing to criminal investigations. As this section discusses, the risk of these and other types of harms are present when data brokers amass and share many different types of information, including financial data, worker data, health data, location, or even publicly available data.

Financial data

With the rise in apps and websites that offer banking services, payment processing, credit monitoring and budgeting support, more companies are obtaining personal financial data online, whether from people directly or by aggregating data from sources such as banks and credit card companies.[4] This data includes names, addresses and other contact information; sensitive data such as payment card and bank account information, dates of birth, and Social Security numbers; and particularly context-specific data such as payment amounts, dates and locations of purchases, merchants involved in a transaction, and other banking activity and transaction history.[5]

Companies like PayPal share people's contact information, bank account and purchase data, and IP addresses with a wide network of third parties for purposes like personalization and marketing.[6] Online retailers – as well as social media companies that have introduced payment

---

[3] Justin Sherman, *Data Brokers and Data Breaches*, Duke Sanford School of Public Policy (Sept. 27, 2022), https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/.

[4] Stan Adams & John Morris, Jr., Center for Democracy & Technology, *Open Banking: Building Trust* (2021), https://cdt.org/wp-content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf; Burt Helm, *Credit Card Companies Are Tracking Shoppers Like Never Before: Inside the Next Phase of Surveillance Capitalism*, Fast Company (May 12, 2020), https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism.

[5] Joseph Cox, *Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans*, Vice: Motherboard (Feb. 19, 2020), https://www.vice.com/en/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous; Center for Democracy & Technology, *Comments Regarding CFPB Inquiry Into Big Tech Payment Platforms*, at 3, (Dec. 20, 2021), https://cdt.org/wp-content/uploads/2021/12/CDT-Comments-to-CFPB-on-Big-Tech-Payment-Systems-Docket-No-CFPB-2021-0017.pdf.

[6] PayPal, *List of Third Parties (Other Than PayPal Customers) With Whom Personal Information May be Shared* (effective Apr. 1, 2023), https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list; Jack Morse, *Payment Apps Collect and Share Your Data. Here's How to Lock Them Down.*, Mashable (June 9, 2021), https://mashable.com/article/venmo-cash-app-paypal-data-privacy.

processing and shopping to their platforms – share people's purchase and browsing activity, location data, and device identifiers, with third-party advertisers, data analytics firms that measure user engagement and advertising performance, and creditors.[7] This financial transaction data is also shared with companies like Yodlee, reportedly one of the largest brokers of financial data, which sells the data to investment and research firms that examine trends in where people spend money.[8]

This data can reveal insights into people's personal activities, habits, and interests. For example, data brokers have categorized people based on their purchases of pregnancy tests or the frequency with which they buy contraceptives, which can reveal information on sexual activity.[9] Data brokers can predict household income based on the types of brands a person buys from, which may indicate how much they are willing to spend on vehicles and other items, or conversely, whether they have lower income or savings that makes them more vulnerable to predatory offers.[10]

In addition, data breaches that expose financial information are particularly likely to lead to identity theft and similar harms.[11] Because data brokers often sell identifiers such as a person's Social Security number along with the person's name, associated addresses, date of birth, and other data, the combined data helps scammers more accurately impersonate the victim.[12] The combined data enables scammers to open new bank or credit card accounts or apply for loans, which can affect the victim's credit score.[13]

---

[7] Amazon, *Amazon.com Privacy Notice* (last updated Jan. 1, 2023), https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ; Meta, *Privacy Policy* (effective July 26, 2022), https://www.facebook.com/privacy/policy/?section_id=2-HowDoWeUse.

[8] Cox, *Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans*, *supra* note 5.

[9] Jon Keegan & Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, The Markup (Jun. 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

[10] *Id.*; Justin Sherman, *How Shady Companies Guess Your Religion, Sexual Orientation, and Mental Health*, Slate (Apr. 26, 2023), https://slate.com/technology/2023/04/data-broker-inference-privacy-legislation.html.

[11] Michelle Hawley, *Is Your Data Really Safe?*, CMSWire (Oct. 6, 2022), https://www.cmswire.com/customer-experience/is-your-data-really-safe/.

[12] Cheryl Winokur Munk, *How to Delete Yourself From the Internet*, CNBC (Feb. 10, 2023), https://www.cnbc.com/2023/02/10/how-to-delete-yourself-from-the-internet.html.

[13] Jessica Roy, *There Are No Perfect Solutions for Identity Theft. But Experts and a Victim Have Ideas*, Los Angeles Times (Oct. 26, 2022), https://www.latimes.com/business/technology/story/2022-10-26/possible-identity-theft-solutions.

Worker data

Data brokers collect an array of information about workers from employers and other sources. Payroll data is one type of worker data that is falling into the hands of data brokers. Equifax's The Work Number claims to receive payroll data from over two million employers every pay period to perform employment and income verification for landlords, banks, and other parties.[14] Debt collectors are also able to buy this data from The Work Number.[15] The company's access to such a large volume of payroll data is particularly concerning, considering that Equifax had a data breach in 2017 that compromised over 147 million consumers' data,[16] and it is unclear what technical data security measures it implements to protect the payroll data it obtains.[17] Newer players in the data broker industry pose similar risks. For example, tech startup Argyle claims to offer more secure access to accurate payroll data and employment history for verification purposes than Equifax does, but Argyle reportedly is behind phishing attempts soliciting workers' workplace login credentials.[18]

Workplace wellness programs are another source for data brokers. Through these programs, third parties partner with employers to collect and analyze data regarding the medications workers take, their existing health conditions, and their personal habits to identify potential healthcare expenses and barriers to workers' productivity.[19] This data may be directly reported by employees or collected from their wearable devices, and the third parties providing these programs may also sell this data to other third parties.[20] When data brokers sell this data to

[14] Chris Chmura, *A Data Broker Has Millions of Workers' Paystubs; See If They Have Yours*, NBC Bay Area (Feb. 9, 2022), https://www.nbcbayarea.com/investigations/consumer/data-brokers-have-millions-of-workers-paystubs-see-if-they-have-yours/2806271/.

[15] *Id.*

[16] John Egan, *Five Years After the Equifax Data Breach, How Safe Is Your Data?*, Bankrate (Sept. 12, 2022), https://www.bankrate.com/finance/credit-cards/how-safe-is-your-data/.

[17] Justin Sherman, *Examining Data Broker Equifax's Relationships with Millions of Employers*, Duke Sanford School of Public Policy (Aug. 24, 2022), https://techpolicy.sanford.duke.edu/blogroll/examining-data-broker-equifaxs-relationships-with-millions-of-employers/.

[18] Joseph Cox, *'Phishing' Sites Buying Workplace Login Details Linked to Well-Funded Startup*, Vice (May 4, 2021), https://www.vice.com/en/article/7kvvbb/argyle-payroll-login-phishing.

[19] Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, *Limitless Worker Surveillance*, 105 Cal. L. Rev. 735, 763 (2017), https://mronline.org/wp-content/uploads/2017/12/3Ajunwa-Schultz-Crawford-36.pdf.

[20] Sally Wadyka, *Are Workplace Wellness Programs a Privacy Problem?*, Consumer Reports (Jan. 16, 2020), https://www.consumerreports.org/health-privacy/are-workplace-wellness-programs-a-privacy-problem-a2586134220/; Ifeoma Ajunwa, *Workplace Wellness Programs Could Be Putting Your Health Data At Risk*, Harvard Business Review (Jan. 19, 2017), https://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk.

marketers, the latter can use it to make inferences about people's stress levels and circumstances and target relevant advertisements accordingly.[21] Insurance companies also use information from data brokers to inform how they sell benefits plans and set premiums, which can affect the benefits employers provide.[22]

Employers' other methods for monitoring workers' activity and productivity might also expose workers' data. Employers implement various methods, including third-party tools, to monitor employees' computer use, what websites they visit, location, movements, communications, and other data.[23] A 2019 survey found that fewer than a third of surveyed corporate executives are confident they are using data being collected in the workplace responsibly, and over half of surveyed workers are worried that their data is at risk.[24] This uncertainty has prompted concerns that as employers' reliance on these third-party tools grows, so will data brokers' access to information collected by these tools.[25]

Health-related data

Commercial apps can help people manage their health, but this has come at the expense of protecting sensitive health data. Health data is not limited to data collected by healthcare providers or insurers – it also includes data collected through mobile fitness and health apps, wearable devices, smart home devices, and other sources by companies whose use and sharing of this data are not subject to the Health Insurance Portability and Accountability Act.[26]

---

[21] Angela Lashbrook, *Your Boss Wants You Healthy For All the Wrong Reasons*, The Outline (Nov. 29, 2018), https://theoutline.com/post/6714/your-boss-wants-you-healthy-for-all-the-wrong-reasons.

[22] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You – and It Could Raise Your Rates*, ProPublica (Jul. 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[23] Matt Scherer, Center for Democracy & Technology, *Warning: Bossware May Be Hazardous to Your Health* (2021), https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/.

[24] Ellen Sheng, *Employee Privacy in the US is At Stake As Corporate Surveillance Technology Monitors Workers' Every Move*, CNBC (Apr. 15, 2019), https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html.

[25] *See* Alistair Simmons, *Fortune 500 Companies' Selling and Sharing of Employee Data*, Duke Sanford School of Public Policy (Feb. 6, 2023), https://techpolicy.sanford.duke.edu/blogroll/fortune-500-companies-selling-and-sharing-of-employee-data/.

[26] Andrew Crawford, Center for Democracy & Technology, *Placing Equity at the Center of Health Care and Technology* 8-10 (2022), https://cdt.org/wp-content/uploads/2022/03/2022-03-22-CDT-Placing-Equity-at-the-Center-of-Health-Care-Technology-final.pdf; Andrew Crawford and Michelle Richardson, Center for Democracy & Technology, *CDT & eHI's Proposed Consumer Privacy Framework for Health Data* (2021), https://cdt.org/insights/cdt-ehis-proposed-consumer-privacy-framework-for-health-data/.

One type of health data at risk is mental health data. Research has found that numerous mental health apps share sensitive data about users' depression, anxiety, suicidality, victimization by domestic violence, disordered eating, post-traumatic stress disorder, and other mental health conditions.[27] A user's mere presence on a mental health website or app, let alone their activity on it, can be a data point shared with other parties to advertise to the user on other websites, without specifying with whom the data is shared.[28] Researchers at Duke University found that data brokers sell people's mental health and medication data with demographic and other non-medical data, grouped into lists such as "Anxiety Sufferers" and "Consumers with Clinical Depression in the United States" to target advertisements related to these mental health conditions.[29] The medication data that is combined with mental health data is sourced from apps like GoodRX, which is used to find prescription discounts and has allegedly shared users' contact information with social media and other companies that target drug advertisements to those users.[30]

Another data broker-related concern is access to and collection and use of reproductive health data, such as data pertaining to abortion in the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*. Reproductive health apps like Flo, Glow, Nurture, and PeriodPlus collect sensitive data about menstrual cycles and pregnancies, including dates when they start and end, related symptoms, weight, and temperature.[31] A 2022 study found that 87 percent of the most popular reproductive health apps share the data they collect with third

[27] Mozilla, *Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security* (May 2, 2022), https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/.
[28] Colin Lecher and Jon Keegan, *Suicide Hotlines Promise Anonymity. Dozens of Their Websites Send Sensitive Data to Facebook*, The Markup (Jun. 12, 2023), https://themarkup.org/pixel-hunt/2023/06/13/suicide-hotlines-promise-anonymity-dozens-of-their-websites-send-sensitive-data-to-facebook; Thomas Germain, *Mental Health Apps Aren't All as Private as You May Think*, Consumer Reports (Mar. 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/.
[29] Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Sanford Cyber Policy Program (2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf.
[30] Natasha Singer, *GoodRX Leaked User Health Data to Facebook and Google, FTC Says*, N.Y. Times (Feb. 1, 2023), https://www.nytimes.com/2023/02/01/business/goodrx-user-data-facebook-google.html; Justin Sherman, *GoodRX, Health Data Brokerage, and the Limits of HIPAA*, Lawfare (Mar. 6, 2023), https://www.lawfareblog.com/goodrx-health-data-brokerage-and-limits-hipaa. .
[31] Samantha Cole, *Here's What Period Tracking Apps Say They Do With Your Data*, Vice (Jun. 28, 2022), https://www.vice.com/en/article/qjkpbq/period-tracking-apps-data-privacy-safety.

parties.[32] With the increasing criminalization of abortion in certain states, sharing reproductive health data puts users of these apps at greater risk from law enforcement and private "bounty hunters."[33] Because it is difficult for people to prevent collection of all data that may reveal their reproductive health care choices, they cannot avoid the risks that come from this data being shared.[34]

Harms arise from the sharing of data regarding other stigmatized conditions as well, which can lead to discrimination and threats of violence. The dating app Grindr, used by members of the LGBTQ+ community, has shared users' HIV status and when they were last tested along with their GPS location data, mobile IDs, and email addresses with two companies hired to optimize the app's performance.[35] Data brokers like MoPub have sold data from Grindr to other data brokers who have resold it, allowing the data to be used by certain buyers to reidentify the app's users.[36] Exposing people's HIV status can especially endanger LGBTQ+ people, who are nearly four times more likely than non-LGBTQ+ people to experience violent victimization.[37]

The sharing of health data can also affect access to insurance and employment, and can expose people to potential scams. A 2021 *New York Times* investigation revealed that thirteen of the twenty health apps that were reviewed each shared health data with an average of three third parties, including for purposes such as generating health-risk prediction scores that are

---

[32] Najd Alfawzan, Markus Christen, Giovanni Spitale, Nikola Biller-Andorno, *Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis*, 10 J. Med. Internet Research mHealth UHealth 189 (2022), https://mhealth.jmir.org/2022/5/e33735/.

[33] Albert Fox Cahn & Eleni Manis, *Surveillance Technology Oversight Project, Pregnancy Panopticon: Abortion Surveillance After Roe* (2022), https://www.stopspying.org/pregnancy-panopticon; Andrew Crawford, Center for Democracy & Technology, *Data After Dobbs: Best Practices for Protecting Reproductive Health Data* (2023), https://cdt.org/wp-content/uploads/2023/05/2023-05-16-CDT-Health-Data-Privacy-Best-Practices-final.pdf; Jake Laperruque, *Cracking Down on Federal Aid for Reproductive Health Surveillance: Fusion Centers* Center for Democracy & Technology (Oct. 5, 2022), https://cdt.org/insights/cracking-down-on-federal-aid-for-reproductive-health-surveillance-fusion-centers/; Jake Laperruque, Eric Null, Andrew Crawford, and Lydia X.Z. Brown, *Following the Overturning of Roe v. Wade, Action is Needed to Protect Health Data*, Center for Democracy & Technology (June 24, 2022), https://cdt.org/insights/following-the-overturning-of-roe-v-wade-action-is-needed-to-protect-health-data/.

[34] Anya E.R. Prince, *I Tried to Keep My Pregnancy Secret*, The Atlantic (Oct. 10, 2022), https://www.theatlantic.com/ideas/archive/2022/10/can-you-hide-your-pregnancy-era-big-data/671692.

[35] Azeen Ghorayshi and Sri Ray, *Gridr is Letting Other Companies See User HIV Status and Location Data*, Buzzfeed (Apr. 2, 2018), https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy.

[36] Shoshana Wodinsky, *Grindr's Data-Sharing Problem is Bigger Than Grindr,* Gizmodo (May 2, 2022), https://gizmodo.com/grindr-shared-location-data-report-1848867990.

[37] Andrew R. Flores, Lynn Langton, Ilan H. Meyer, and Adam P. Romero, *Victimization Rates and Traits of Sexual and Gender Minorities in the United States: Results from the National Crime Victimization Survey, 2017* (2020), https://www.science.org/doi/10.1126/sciadv.aba6910.

provided to life insurance companies to identify prospective customers.[38] As discussed earlier, people's health data is also shared with certain employers that use it to strategize on how to reduce their expenses on employee health benefits.[39] Data brokers have also used data of elderly people and people with Alzheimer's disease to create lists of people who are more vulnerable to scams.[40]

Third-party sharing of health data is widespread. In a 2021 report, the International Digital Accountability Council assessed privacy risks of 152 digital health apps and found that 39 apps transmit users' advertising identifiers to at least one third-party endpoint not disclosed in their privacy policies, with 28 apps sending multiple identifiers to third parties.[41] An earlier University of Pennsylvania study examined 538 websites that provided information and resources regarding COVID-19 – including government and academic websites – and found that 99 percent included third-party data requests and 89 percent included third-party cookies.[42] A new report found a database of 650,000 labels that data brokers across the globe derived from sensitive data, especially data from which physical or mental health needs or interests can be inferred, to be used by advertising companies.[43]

Location data

Location data can include general neighborhoods or specific landmarks that a person visits, or more detailed GPS data from the paths they travel. In addition to health data, the *New York*

---

[38] Thorin Klosowski, *We Checked 250 iPhone Apps – This is How They're Tracking You*, N.Y. Times: Wirecutter (May 6, 2021), https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/.

[39] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?*, Wash. Post (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

[40] Alistair Simmons, *The Justice Department's Agreement With a Data Broker That Facilitated Elder Fraud*, Lawfare Blog (Nov. 7, 2022) https://www.lawfareblog.com/justice-departments-agreement-data-broker-facilitated-elder-fraud.

[41] Holden Williams, Ginny Kozemczak, and Dan Kinney, Int'l Digital Accountability Council, *Digital Health is Public Health: Consumers' Privacy & Security in the Mobile Health App Ecosystem* (2021), https://digitalwatchdog.org/wp-content/uploads/2022/01/Digital-Health-is-Public-Health-Consumers-Privacy-and-Security-in-the-Mobile-Health-App-Ecosystem.pdf.

[42] Matthew S. McCoy, Timothy Libert, David Buckler, David T. Grande, and Ari B. Friedman, *Prevalence of Third-Party Tracking on Covid-19-Related Web Pages*, J. American Medical Association (2020), https://jamanetwork.com/journals/jama/fullarticle/2770565; Michele W. Berger, *What Can Browser History Inadvertently Reveal About a Person's Health?*, University of Pennsylvania: Penn Today (Apr. 29, 2022), https://penntoday.upenn.edu/news/what-browser-history-inadvertently-reveals-Penn-CMU-digital-health-privacy-initiative.

[43] Keegan, *supra* note 9.

Times' investigation mentioned above found that numerous shopping, news, dating, and weather apps gather location data to provide necessary app functions, but also share this data to enable devices to be tracked for advertising purposes.[44] Location data is also collected by apps that have no need for it, which transmit this data through software development kits that data brokers pay to have app developers include within these apps.[45] Mobile carriers are another source of location data, which has been shared with bounty hunters and stalkers, prompting a Federal Communications Commission inquiry into large mobile providers about their location data-sharing practices.[46]

Aside from advertising, location data is also shared to gain insights into people's private activities.[47] One data broker, Outlogic (formerly X-Mode), reportedly has gathered location data from multiple Muslim prayer apps, multiple dating apps, the family safety app Life360, and other sources, and has sold that data to several parties, including military contractors and other companies that provide services to government entities.[48] Another data broker, Kochava, allegedly sold precise geolocation data about millions of mobile devices that allowed entities to track people's "movements to and from sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at risk populations, and substance use recovery."[49] Data about a person's movements to a sensitive location and how much time they spent there can be combined with data regarding other places a person has visited, as well as their search, browsing, and purchase history, to paint an increasingly detailed picture of their activities.[50]

---

[44] Klosowski, *supra* note 38.
[45] Sherman, *How Shady Companies Guess Your Religion, Sexual Orientation, and Mental Health*, *supra* note 10.
[46] Joseph Cox, *T-Mobile 'Put My Life in Danger' Says Woman Stalked With Black Market Location Data*, Vice: Motherboard Aug. 21, 2019, https://www.vice.com/en/article/8xwngb/t-mobile-put-my-life-in-danger-says-victim-of-black-market-location-data ; Federal Communications Commission, *Rosenworcel Probes Mobile Carriers on Data Privacy Practices*, Jul. 19, 2022, https://www.fcc.gov/document/rosenworcel-probes-mobile-carriers-data-privacy-practices.
[47] Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, Brookings (July 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights.
[48] Johana Bhuiyan, *Where Does Your Info Go? US Lawsuit Gives Peek into Shadowy World of Data Brokers*, The Guardian (Mar. 23, 2022), https://www.theguardian.com/technology/2022/mar/23/data-brokers-lawsuit-security-transparency; Joseph Cox, *How the U.S. Military Buys Location Data From Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
[49] Complaint, Federal Trade Commission v. Kochava, No. 2:22-cv-377 (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
[50] Crawford, *Data After Dobbs: Best Practices for Protecting Reproductive Health Data*, *supra* note 33.

Data scraped from publicly available sources

Data brokers can readily access and collect any data on the internet that is publicly viewable or anything that is contained in a public record, such as real estate or voter registration data. Publicly available data can include certain financial, worker, health, location, and other data. LexisNexis and Thomson Reuters are among the most prolific data brokers compiling and selling large quantities of personal data and the inferences they make from this data to both private and public sector entities.[51] LexisNexis' Accurint and Thomson Reuters' CLEAR products compile publicly available information, license plate data, Social Security numbers, and more, which law enforcement authorities have allegedly used to target immigrant communities and punish immigration activists.[52] Other data brokers include people-search platforms like Spokeo, which provides personal data combined with publicly available data. The company claims to take proactive steps to prevent use of the data to facilitate violence, such as requiring users to self-report how they intend to use its service.[53] However, like other people-search platforms, it reportedly provides paid access to people's email and mailing addresses and other data and has acknowledged challenges in its opt-out process.[54] The continued availability of such data online can enable abusers to stalk victims of intimate partner violence.[55]

Data shared by these data brokers can have harmful ramifications, particularly when it is inaccurate or incomplete, because background checks that rely on this data can adversely affect housing, employment, and other critical decisions.[56] For instance, background checks include data gleaned from public court indexes, which indicate when someone has been charged with a crime or has had an eviction filed against them.[57] However, these data points do not

---

[51] Sarah Lamdan, *The Quiet Invasion of 'Big Data'*, Wired (Nov. 9, 2022), https://www.wired.com/story/big-information-relx-privacy-surveillance-data/.
[52] *Id.*; *LexisNexis Illegally Collected and Sold People's Personal Data, Lawsuit Alleges*, CBS News (Aug. 16, 2022), https://www.cbsnews.com/news/lexisnexis-lawsuit-collected-sold-personal-data-immigration-advocates- allege/.
[53] Tonya Riley, *People Search Websites Create Privacy Nightmares for Abortion Rights Advocates*, Cyberscoop (Sept. 29, 2022), https://cyberscoop.com/data-broker-removal-services-find-new-demand/.
[54] Mara Hvistendahl, *I Tried to Get My Name Off People-Search Websites. It Was Nearly Impossible*., Consumer Reports (Aug. 20, 2020), https://www.consumerreports.org/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly--a0741114794/.
[55] *Id.*
[56] Aditi Shrikant, *This Common Problem With Tenant Background Checks is Costing Renters*, CNBC (Nov. 17, 2022), https://www.cnbc.com/2022/11/17/background-checks-are-often-inaccurate-make-renting-more-expensive.html.
[57] Lauren Kirchner, *Data Brokers May Report COVID-19-Related Evictions for Years*, The Markup (Aug. 4, 2020), https://themarkup.org/locked-out/2020/08/04/covid-evictions-renter-background-reports.

demonstrate the person's culpability with respect to these legal proceedings – a charge does not mean the person was convicted, and an eviction filing does not mean the person was ultimately evicted.[58] Nevertheless, background screening companies, and the companies they serve, often use this information to make adverse decisions about those people.

II. The sprawling and opaque data broker ecosystem undermines accountability.

Data sold by data brokers can be combined with other data, repurposed for a range of new uses, and/or shared with a network of third parties that people would not reasonably expect. People have little visibility into which data brokers obtain their data, from whom their data is obtained, to whom their data is sold, and to what additional uses it is put. Thus, the sheer breadth and opacity of data sharing makes it impossible for people to trace how widely their data has been accessed and used, let alone to completely scrub their data from every entity that has obtained it.[59]

The ability to opt out of certain data broker practices does not provide consumers with effective ability to control access to, sharing, and use of their data.

While it is helpful for a data broker to enable consumers to opt out of the entity's sharing or sale of data, the opt-out process is inadequate. As an initial matter, because data brokers are in many cases third parties with which a consumer has no direct relationship, the consumer often will be unaware that a particular broker has access to their data. As a result, they would have no reason to exercise any opt out rights with that broker or even know that they should consider doing so. Further, the option to opt out puts all the burden on the consumer rather than those profiting from the data[60] – that is particularly unfair when the consumer had no intention or expectation of sharing data with a broker in the first place and obtains no benefit from the broker having the data.

---

[58] Bill Block, *How Biased Algorithms Create Barriers to Housing*, ACLU Washington (Feb. 16, 2022), https://www.aclu-wa.org/story/how-biased-algorithms-create-barriers-housing; Rasheedah Phillips, *Eviction Records Follow People Around for Years. This Isn't Fair.*, (June 4, 2021), https://nextcity.org/urbanist-news/eviction-records-follow-people-around-for-years-this-isnt-fair.

[59] Winokur Munk, *supra* note 12.

[60] For example, various services are available to submit opt-out requests on people's behalf on an ongoing basis. Consumers still have to find each individual data broker that has their information and initiate opt-out requests for each. *See* National Network to End Domestic Violence, *Data Brokers: What They Are and What You Can Do About Them* (last updated 2022), https://www.techsafety.org/data-brokers; Consumer Reports, *Permission Slip: FAQ*, https://permissionslipcr.com/faq.php.

Further, even if a consumer does exercise an opt out right, it does not always lead to people's data being removed promptly, nor does it prevent data brokers from re-acquiring people's data from the original or newer sources.[61] And Consumer Reports also warns that companies might not fulfill opt-out requests.[62]

Deidentified, anonymized, and even aggregated data could be reidentified.

Deidentification, anonymization, and aggregation can help prevent harms from data sharing, but only to an extent. Deidentification and anonymization often do not prevent reidentification, which can be accomplished through a combination of location data, search histories, demographics, and other data.[63] Reports have found that connecting just a couple of location data points in a large anonymized dataset can indicate a trajectory that is unique enough to identify a person.[64] When shared and repurposed, this combined data can facilitate inferences that would harm marginalized people. For example, when a Grindr user's location data shows they visited a venue catering to LGBTQ+ communities, and data brokers share this data to target LGBTQ+-related advertisements to the user's device, the user could be outed to anyone who is able to view the device.[65]

After Life360 was reported to have sold its users' location data to data brokers, it announced that it would "sell only precise location data to Arity and 'aggregated' location data to PlacerAI"

---

[61] *Id.*; Yael Grauer, *What Are Data Brokers and Why Are They Scooping Up Information About You?*, Vice (Mar. 27, 2018), https://www.vice.com/en/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

[62] Consumer Reports, *supra* note 60.

[63] Justin Sherman, *Big Data May Not Know Your Name. But It Knows Everything Else.*, Wired (Dec. 19, 2021), https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/.

[64] Ali Farzanehfar, Florimond Houssiau, and Yves-Alexandre de Montjoye, *The Risk of Reidentification Remains High Even in Country-Scale Location Datasets*, 2 Patterns (2021), https://www.sciencedirect.com/science/article/pii/S2666389921000143; Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[65] Sarah Syed, Natalia Drozdiak, & Nate Lanxon, *Grindr Shares Location, Sexual Orientation Data, Study Shows*, The Detroit News (Jan. 14, 2020), https://www.detroitnews.com/story/business/2020/01/14/grindr-shares-location-sexual-orientation-data-study-shows/40997573/; Chris Wood, Katelyn Ringrose, Carlos Gutierrez, Amie Stepanovich, & Connor Colson, LGBT Tech and Future of Privacy Forum, *The Role of Data Protection in Safeguarding Sexual Orientation* 9, 13 (2022), https://www.lgbttech.org/_files/ugd/1b643a_21883c316e1547c99c6a1d997688f975.pdf.

going forward.[66] This is an improvement to the company's more widespread sale of location data, especially considering that aggregation is a more privacy-protective measure than de-identification or anonymization. However, aggregation is not foolproof, either – the smaller the aggregated dataset, the easier it is to reidentify a person's data within that dataset.[67] For instance, one could "aggregate" data across a zip code containing only a few residents, but then that aggregate data would be fairly indicative of those residents.

An inconsistent approach to disclosure limits understanding of how widely data is shared.

Companies often provide "disclosure" regarding their data sharing by using vague or onerously lengthy privacy policies that bury their explanations about how and why consumer data is shared with third parties such as data brokers. Being adequately informed about a company's data-sharing practices might help a person decide whether to trust that company's website or app. However, making that determination for every website and online service a user visits is an onerous task. Moreover, an individual should not be in a position where they are forced to permit their data to be shared with a data broker in order to use a site or service. That is all the more true given that it is not just certain websites or apps that share data with data brokers – even internet service providers and antivirus companies often share online users' data with third parties, so people's data is at risk the moment they go online. For example, Comcast and AT&T's privacy policies explain that they share customers' personal data with third parties, including credit reporting agencies; service providers that perform marketing, user analytics, and identity verification functions; and third-party advertising partners.[68] During installation of Avast's antivirus software, the company provides a pop-up that asks users whether they consent to sharing their data and informs users that their data will be deidentified and aggregated, but does not mention how their data can be retained and reidentified – users can only learn of the latter by perusing the company's privacy policy.[69] Further, companies' privacy policies may not identify the data brokers that obtain users' data, and, as noted above, data brokers typically do

[66] Jon Keegan & Alfred Ng, *The Popular Family Safety App Life 360 is Selling Precise Location Data on Its Tens of Millions of Users*, The Markup (Dec. 6, 2021), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

[67] Luk Arbuckle, *Aggregated Data Provides a False Sense of Security*, International Association of Privacy Professionals (Apr. 27, 2020), https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/.

[68] Comcast Xfinity, *Our Privacy Policy Explained* (effective Oct. 12, 2021), https://www.xfinity.com/privacy/policy#privacy-who; AT&T, *AT&T Privacy Policy* (effective June 6, 2022), https://about.att.com/privacy/full_privacy_policy.html.

[69] Michael Kan, *The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks*, PCMag (Jan. 27, 2020), https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks.

not interact with users directly. Therefore, as difficult as it may be for users to thoroughly understand the data practices of the first parties to whom they provide their data, users are even less likely to read data brokers' privacy policies.

As the RFI notes, data broker registries are one tool to increase disclosure, though they currently vary in the level of insight they offer. California and Vermont have established data broker registries that each provide information to the public on hundreds of data brokers.[70] A search for the same data broker on each registry produces different degrees of detail, and some data brokers only appear on one registry. California's registry asks for fewer details, specifically how consumers can submit opt-out, deletion, and other requests. In contrast, Vermont's registry asks about the opt-out method, limitations and exceptions to the opt-out, data brokers' assessment of the purpose for which data is purchased, number of data breaches in the past year and consumers affected, knowledge that minors' data was collected, and any additional details data brokers would like to provide. In either registry, the usefulness of each registry entry depends on the amount of information the data broker reports, and on people knowing which data broker to search.

Texas also recently passed a law requiring data brokers to register with the state.[71] Like California's data broker registry law, Texas's law does not apply to entities that are consumer reporting agencies to the extent that they are covered by the FCRA.[72] Therefore, while state-level data broker registries provide people with some information about the companies that may access their data, their inconsistent reporting requirements and coverage of entities that sell data makes them an insufficient vehicle for providing information to users and preventing harm.

Harm to consumers is exacerbated by government evasion of legal requirements through purchases of data from data brokers.

To make matters worse, while the Fourth Amendment requires government entities to obtain a warrant to collect data in which people have a reasonable expectation of privacy, law

[70] California Department of Justice, https://oag.ca.gov/data-brokers; Vermont Secretary of State, https://bizfilings.vermont.gov/online/DatabrokerInquire/DataBrokerSearch.
[71] Texas Senate Bill 2105.
[72] Cal. Civ. Code §1798.99.80(d)(1); Texas Senate Bill 2105 §509.003(b)(5).

enforcement and national intelligence agencies can buy or collect publicly available data.[73] As a result, their acquisition of data hinges on their definitions of "publicly available" data.[74] For example, the Attorney General guidelines for the Office of the Director of National Intelligence's (ODNI) data practices state that publicly available data includes data that is accessible online to the public and data that is available to the public by subscription or purchase.[75] It also includes commercially acquired data that non-government entities, including private-sector purchasers, could acquire in the same manner as government entities from the same commercial source.[76]

A recently declassified ODNI report acknowledged that government agencies' purchases of increasingly vast amounts of "commercially available information" have far surpassed what has traditionally been considered publicly available data.[77] ODNI's report states that commercially available information is less strictly regulated than data exclusively available to governments because the former is considered publicly available information.[78] However, the report explains that commercially available information has reached "a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection, and that could be used to cause harm to an individual's reputation, emotional well-being, or physical safety."[79] For instance, the Department of Homeland Security reportedly buys location data from data brokers to avoid having to secure a warrant for such data.[80] State and local governments also contract with data brokers like Fog Data Science, which has made its collection of location data available to several law enforcement agencies at all levels of

[73] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, Center for Democracy & Technology, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers* 19 (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.
[74] *Id.* at 20-21.
[75] Office of the Director of National Intelligence, *Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive Order 12333* (2020), https://www.intel.gov/assets/documents/702%20Documents/declassified/AGGs/ODNI%20guidelines%20as%20approved%20by%20AG%2012.23.20_OCR.pdf.
[76] *Id*.
[77] Wes Davis, *US Spy Agencies Are Buying the Same Surveillance Data Advertisers Crave*, The Verge (Jun. 14, 2023), https://www.theverge.com/2023/6/14/23759585/odni-spy-report-surveillance-data-location-tracking; Office of the Director of National Intelligence, *Senior Advisory Group Panel on Commercially Available Information* (2022), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [hereinafter "ODNI Report"].
[78] ODNI Report, *supra* note 77, at 8.
[79] *Id.* at 24.
[80] Corin Faife, *Feds Are Tracking Phone Locations With Data Bought From Brokers*, The Verge (Jul. 18, 2022), https://www.theverge.com/2022/7/18/23268592/feds-buying-location-data-brokers-aclu-foia-dhs.

government.[81] Disclosure only goes so far when the volume of data available to and sold by data brokers to private and government entities alike remains unaffected.

III. The CFPB should continue to clarify how the FCRA applies to data sharing and selling by brokers.

The CFPB should use its authority to clarify that the FCRA applies to many of the data sharing activities of data brokers. The FCRA governs consumer reports, which are any communications of information by a consumer reporting agency that bears on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, and which are used or expected to be used in whole or in part for certain permissible purposes enumerated by the law.[82] There can be no question that much of the information shared by data brokers, from financial data to information about a person's online activities, bears on factors such as a consumer's creditworthiness, personal characteristics, and reputation.

Moreover, that information is used or can be expected to be used at least in part for the permissible purposes set out in the FCRA such as for employment purposes or in connection with credit or insurance underwriting. For example, data brokers like Verisk sell behavioral data along with vehicle data and personally identifying data such as phone numbers and addresses they collect from smart home and mobile devices to inform risk evaluations for life, auto, and property insurance products.[83] Insurers can repurpose data collected from these devices to terminate coverage or increase premiums.

Because they at least in part regularly assemble and communicate information to third parties that is used or expected to be used as a factor in determining eligibility for credit, insurance,

---

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

[82] 15 U.S.C. §1681a(d).

[83] Verisk, *Internet of Things and Telematics Solutions*, https://www.verisk.com/insurance/capabilities/telematics/; Jon Keegan and Alfred Ng, *Who is Collecting Data From Your Car*, The Markup (Jul. 27, 2022), https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car; Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke U. Sanford Cyber Policy Program 6-7 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

employment, or other permissible purpose authorized under the FCRA and are compensated for doing so, data brokers often act as consumer reporting agencies subject to the FCRA.[84]

The CFPB should clarify ways in which the FCRA imposes limits and obligations on data broker activities. It already has addressed one such restriction by issuing an interpretive rule advising that furnishing data under the FCRA is only permissible with respect to the consumer whose data is the subject of the data user's request.[85] In doing so, the CFPB recognized that whether a consumer's data is being furnished for a permissible purpose is an individualized inquiry specific to that consumer. The CFPB should affirm explicitly that companies subject to the FCRA violate it when they furnish multiple people's data at one time.

In addition, the FCRA requires reasonable procedures to assure the maximum possible accuracy of information in consumer reports.[86] The CFPB should make clear that a data broker acting as a consumer reporting agency violates the Act when it fails to verify the accuracy of the data it furnishes as part of a consumer report.

The CFPB should also emphasize the applicability of current restrictions on sharing data for permissible purposes related to employment to data brokers subject to the FCRA. Under the FCRA, a consumer report furnished for "employment purposes" is a report used to evaluate a consumer for employment, promotion, reassignment, or retention as an employee.[87] The FCRA requires written authorization from consumers for an entity to obtain their consumer report for employment purposes.[88] The FCRA also requires that when an adverse action is taken based on a consumer report, a copy of the report must be provided to the consumer.[89] This requirement applies to the use of consumer reports to make any decision for employment purposes that adversely affects any current or prospective employee.[90]

The CFPB should also clarify that the FCRA generally prohibits data brokers from sharing health data in consumer reports. The FCRA defines "medical information" to include data created by or derived from a consumer that relates to their past, present, or future physical, mental, or behavioral health; the provision of health care to the consumer; or the payment for provision of

[84] 15 U.S.C. §1681a(f).
[85] 87 Fed. Reg. 41243.
[86] 15 U.S.C. §1681e(b).
[87] 15 U.S.C. §1681a(h).
[88] 15 U.S.C. §1681b(2).
[89] 15 U.S.C. §1681b(3).
[90] 15 U.S.C. §1681a(k)(1)(b).

health care to the consumer.[91] The FCRA allows this data to be included in a consumer report only to the extent that it (1) is in connection with an insurance transaction with the consumer's affirmative consent, (2) is relevant to carry out an employment purpose or credit transaction with the consumer's written consent, or (3) pertains solely to medical debts.[92] The FCRA prohibits anyone receiving medical information for employment, credit, or insurance purposes from disclosing it to another party except as necessary to carry out the purpose for which they initially received the information or as allowed by federal law relating to medical confidentiality.[93] The CFPB should make clear that data brokers' acquisition and sale of health data is generally beyond the scope of permitted sharing of medical information under the FCRA.

Conclusion

The CFPB has demonstrated leadership in scrutinizing the evolving data practices through which data brokers exploit consumers. Data brokers have been able to take advantage of the growing, obscure ecosystem of data sharing and sale to evade accountability. The CFPB should exercise its authority through interpretive rules, advisory opinions, and similar efforts to clarify when data brokers' compilation and sale of personal data is subject to the obligations and remedies under the FCRA.

[91] 15 U.S.C. §1681a(i).
[92] 15 U.S.C. §1681b(g)(1).
[93] 15 U.S.C. §1681b(g)(4),(6).