epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CONSUMER FINANCIAL PROTECTION BUREAU

Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information

88 Fed. Reg. 16,951

July 14, 2023

Table of Contents

I. Introduction

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Consumer Financial Protection Bureau (CFPB)'s recent Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information published on March 21, 2023.[1]

Data brokers can and should be regulated under the FCRA, CFPA, and similar laws, and EPIC urges the CFPB to adopt an expansive definition of data broker misconduct to capture the variety of harmful activity that data brokers undertake; shift the regulatory burden from individual consumers exercising their rights to data brokers and other entities profiting off harmful data collection and use; coordinate efforts with the FTC to prioritize data minimization and data security within its regulations; and clarify its interpretations of FCRA provisions and definitions using illustrative examples.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has long advocated for robust safeguards to protect consumers from exploitative data collection, use, distribution, and retention practices, including data minimization restrictions under which data can only be collected, used, or disclosed as necessary, consistent with the reasonable expectations of the consumer.[3] EPIC has also fought for greater oversight into how companies and government agencies

[1] Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16,951 (June 13, 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] *About Us*, EPIC, https://epic.org/about/ (2023).
[3] *See*, *e.g.*, Consumer Reps. & EPIC, How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking (2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/ [hereinafter "CR EPIC Data Minimization Whitepaper"].

target individuals based on data collected about those individuals,[4] greater transparency regarding the lifecycle of collection and disclosure of Americans' personal data,[5] and more robust regulatory enforcement to safeguard the rights of consumers.[6]

EPIC's comment, which responds to questions throughout the CFPB's Request for Information, is organized into the following topics: the data lifecycle and business of data brokers; the negative impacts of ubiquitous commercial data collection on consumers; the insufficiency of existing regulations and mechanisms to constrain harmful data broker practices and protect consumers; and specific recommendations for the CFPB. We are available to discuss any aspect of our comment with the CFPB and welcome any questions you may have.

II. The Data Lifecycle and Business of Data Brokers

a. The range of data bought and sold on the data broker market

The following is responsive to Questions 1-3.

Simply put, data brokers collect, access, process, organize, and sell ***a lot*** of personal data. Data brokers sell a wide variety of personal data elements and datasets filtered and organized by demographic or descriptive categories. In addition to collecting and selling raw data, many data brokers also market assessments, risk scores, and other inferences that purport to help entities make decisions or recommendations.[7]

---

[4] *See, e.g., Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors: Hearing Before the H. Comm. on House Admin.*, 117th Cong. 53 (2022), https://epic.org/documents/hearing-on-big-data-privacy-risks-and-needed-reforms-in-the-public-and-private-sectors/ (statement of Caitriona Fitzgerald, Deputy Director, EPIC).

[5] *See, e.g.*, EPIC, Comments on CFPB Inquiry into Big Tech Payment Platforms, 86 Fed. Reg. 61182 (Dec. 21, 2021), https://epic.org/documents/epic-comments-on-cfpb-inquiry-into-big-tech-payment-platforms/.

[6] *See, e.g.*, EPIC, Comments on CFPB Request for Information on the Equal Credit Opportunity Act and Regulation B, 85 Fed. Reg. 46600 (Oct. 2, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CFPB-Oct2020-AI-ML.pdf.

[7] *See, e.g., CLEAR Risk Inform*, Thomson Reuters (last visited July 10, 2023), https://legal.thomsonreuters.com/en/products/clear-investigation-software/clear-risk-inform; *Credit Risk Assessment and Management*, LexisNexis Risk Solutions (last visited July 10, 2023),

To illustrate both the breadth and depth of the data broker industry, EPIC provides the following of the types of data and "insights" data brokers offer to purchasers. Of course, due to the lack of full transparency into the data broker market, this list is necessarily non-exhaustive:

- First and last name
- Date of birth/exact age
- Income information
- Gender
- Marital status
- Single parent status
- Ethnicity/race
- Residential address[8]
- Whether someone has an account on Grindr or a Muslim prayer app, for example[9]
- Home market value
- Credit score
- Homeowner status
- Number of people in an individual's household
- Neighborhood characteristics
- Net worth
- Information about an individual's children
- Drivers license information
- Social security number
- Whether an individual is a state government worker
- Whether an individual is an active living Jew
- Whether an individual is a wealthy senior near retirement
- What is in an individual's shopping cart (e.g., grocery information, other purchases considered)
- Religion
- Language
- Profession
- Degrees held and education
- Pets
- Exercise habits

---

https://risk.lexisnexis.com/corporations-and-non-profits/credit-risk-assessment. For more on the impact of data-broker risk scoring offerings, *see, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 8–17 (2014).

[8] Privacy Bee, *These Are the Largest Data Brokers in America*, Privacy Bee (2023), https://privacybee.com/blog/these-are-the-largest-data-brokers-in-america/.

[9] *See* 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; Matt O'Brien & 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.

- Bankruptcy history
- Criminal records
- Credit card transactions/purchasing behavior
- Location data
- Smart phone app usage (e.g., clicks, swipes, video views, registrations, app installs, likes, locations, sharing, posting, purchases, calls)
- Credit history
- Information from public records or newspaper notices (e.g., court records, voter records, vehicle records, name and address changes, marriages, divorces)
- Newspaper and magazine subscriptions
- Website data (e.g., browsing and usage data)
- Prescriber information (e.g., name, Pill Identifier number, Drug Enforcement Agency number, age, email address, telephone number, allowed to contact or not)
- General hospital systems data (e.g., number of procedures performed, departmental data)
- Health score
- Risky health behavior data
- BMI estimate
- An individual's expected ability to pay for health care based on demographic characteristics (e.g., millennials aged 18-42 years with a low expected ability to pay for medical expenses or Gen X and young Boomers ages 43-64 years with a medium expected ability to pay for medical expenses)
- Hospital readmission risk score
- Medication adherence score
- Total cost risk score (e.g., how much the individual is expected cost to the healthcare system over the next few months)
- Information on mental health conditions and prescriptions (e.g., depression, attention disorder, insomnia, anxiety, medication and treatments for ADHD/ADD, antidepressants, bipolar disorder)
- Information on other medical conditions (e.g., diabetes, allergies, dementia or Alzheimer's Disease, heart problems, bladder control difficulties, frequent headaches, high blood pressure)
- Likelihood of having depression
- Likelihood of having anxiety
- Health plan enrollment
  Medical events
- Clinical facilities an individual has been served by or at (e.g., surgery centers, imaging centers, health clinics, long term facilities, hospitals/IDNs, connected care organizations)
- Lab data, genomic data, and biomarkers
- Physician profiles and physician groups (e.g., general practice, addiction specialists)
- Data from patient/disease registries, wearables/connected devices, and patient support/management programs
- Location data related to reproductive health services
- Data on how many prescriptions for each medication were filled in a given zip code or area
- EMR data (electronic medical records)

- Property tax assessments
- Global watch lists
- Aircraft/watercraft registration
- Accident reports
- College attendance records
- Likelihood of living in a high crime area
- Likelihood of being food insecure or living in a food desert
- Likelihood of having access to transportation[10]
- Burdened by Debt: Singles
- Mid-Life Strugglers: Families
- Resilient Renters
- Very Spartan
- X-tra Needy
- Zero Mobility
- Hard Times
- Enduring Harships
- Humble Beginnings
- Struggling Elders
- Retiring on Empty
- Tough Start: Young Urban Single Parents
- Credit Crunched: City Families
- Meager Metro Means
- Relying on Aid: Retired Singles
- Rough Retirement: Small Town and Rural Seniors
- Financial Challenges
- Credit Reliant
- Rocky Road
- Very Elderly
- Ethnic Second-City Strugglers
- Fragile Families
- Rural and Barely Making It[11]

This data is used in a staggering variety of ways, depending on the party that purchases it and their reasons for doing so.

[10] Joanne Kim, Duke Sanford Cyber Pol'y Program, *Data Brokers and the Sale of Americans' Mental Health Data* 20–21 (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.
[11] Staff of S. Comm. on Com., Sci., & Transp., *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purpose*s at ii (Dec. 18, 2013), https://www.commerce.senate.gov/services/files/0D2B3642-6221-4888-A631-08F2F255B577.

b. The participants and victims of the data broker market

The following is responsive to Questions 4, 5, and 12.

There are many different types of entities that purchase datasets from data brokers, including government entities, political entities, commercial entities, non-profit entities, and individuals. EPIC provides an illustrative list of examples of data broker relationships (**bolded**), and how they have played out between different kinds of entities:

- Catholic News Outlet *The Pillar* (**buyer**) purchased location data from an unnamed data broker (**seller**), which itself obtained that data from the dating app Grindr (**data provider**). *The Pillar* then published and shared some of that information with the U.S. Conference of Catholic Bishops**.** *The Pillar*'s reporting outed a priest as gay and led to his harassment (**victim**).[12]

- Multiple sources have detailed how data brokers (**sellers**) traffic in location data. This includes location data that may reveal reproductive health choices, which anti-abortion groups (**buyers**) have used it to target or dox someone for having an abortion (**victim**) or to target anti-abortion ads to people sitting in clinics.[13]

- Fog Data Science (**seller/broker**) provides "risk predictions" and data to U.S. intelligence agencies and law enforcement agencies (**buyers**) and claims that it is "capable of delivering both forensic and predictive analytics and near real-time insights on the daily movements of the people identified with those mobile devices as they engage with signals spread across locations both US and throughout the world." In 2019, Fog Data Science boasted that its platform processed "250 million devices each month, 15 billion location signals each day, 10 million fenced points of interest" and more than 1 million daily events.[14]

[12] Matt O'Brien & 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.
[13] Joseph Cox, *Data Broker is Selling Location Data of People Who Visit Abortion Clinics*, Vice (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.
[14] Memorandum from Chino Police Detective Jason Larkin on the Chino Police Contract with Fog Data Science 25 (Oct. 10, 2019), https://www.documentcloud.org/documents/22187494-chino_2019-20_attachments#document/p25/a2143086.

c. The use of data purchased on the data broker market to train proprietary algorithms

The following is responsive to Question 7.

To develop and refine proprietary algorithms, companies engage in direct data collection, indirect data collection, and the purchase of raw data and inferences (either outright or through licensed access). Notably, companies also develop and use proprietary algorithms to collect and scrape information from the internet and other sources.

Opacity is common (and to some extent inherent) in the development of proprietary algorithms. But marketing materials from Lusha, a registered data broker and lead generation platform, illustrate some of the ways the company uses a proprietary algorithm to create individualized business profiles of professionals.[15] Lusha outlines how it obtains data from users' emails that it "license[s] information from business partners . . . that utilize the most cutting-edge AI and machine learning technology to collect data from public records, publicly available information, and business directories;" that its "proprietary algorithm scans publicly available sources and retrieves public information with advanced tools;" and that its uses "big data technology [to] identif[y] the most up-to-date information for each Business Card and simultaneously removes any outdated information from the system."[16] As the example of Lusha reveals, brokers collect data from disparate sources to glean insights and train algorithms that they can use or market separately.

d. The lack of meaningful controls on the data broker market

The following is responsive to Questions 18 and 19.

Data brokers rarely impose adequate controls on who can purchase information on the data broker market.[17] And because there is no direct relationship between the consumer and data broker,

---

[15] *Our Data Sources*, Lusha, https://www.lusha.com/our-data/ (last visited July 11, 2023).
[16] *Id.*
[17] Justin Sherman, Duke Sanford Cyber Pol'y Program, Data Brokers and Sensitive Data on U.S. Individuals 11 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

the consumer has no meaningful way to either be informed as to the accuracy of the data in their profile or to control it. The sheer amount of data generated online every minute of every day creates a race to collect as much as possible without regard to need or accuracy.[18]

There is also a widespread lack of technical and administrative controls on the accuracy of data trafficked on the data broker market. As just one example, when data brokers cannot obtain verified information to fill out a consumer's profile, brokers may rely inferences and best guesses to fill in the gaps. When one prominent broker, Experian, "can't find a source of verified data," it simply "uses statistical models to guess personal attributes, including political preferences, financial health and which types of products someone is likely to buy."[19] This introduces additional inaccuracy into the data broker ecosystem.

e. The harmful impact of data brokers on consumer autonomy

The following is responsive to Question 6.

The data broker ecosystem limits consumer autonomy by shaping purchasing preferences and patterns. Commercial surveillance practices require constant data collection, fueling data brokers' ability to create and sell extremely detailed profiles and analytics about consumers. Thousands of data brokers amass millions of data points that can be combined, shared, and analyzed along with

[18] *See, e.g.*, Charles Street, *How Data Brokers Steal & Sell Your Identity and How You Can Stop It*, Priv. Hub (June 7, 2023), https://www.cyberghostvpn.com/en_US/privacyhub/data-brokers-put-a-price-tag-on-your-privacy-and-then-sell-it/; Olivia Terragni, *Data Brokers: How Law Enforcement Rely on Inaccurate Data to Supplement Investigations*, Red Hot Cyber (June 15, 2022), https://www.redhotcyber.com/en/post/data-brokers-how-law-enforcement-rely-on-inaccurate-data-to-supplement-investigations/; Douglas MacMillan, *Data Brokers Are Selling Your Secrets. How States are Trying to Stop Them.*, Wash. Post (June 24, 2019), https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/; John Lucker et al., *Predictably Inaccurate*, 21 Deloitte Rev. 8 (2017), https://www2.deloitte.com/content/dam/insights/us/articles/3924_Predictably-inaccurate/DUP_Predictably-inaccurate-reprint.pdf; John Lucker, *Predictably Inaccurate: Big Data Brokers*, LinkedIn Pulse (Nov. 18, 2014), https://www.linkedin.com/pulse/20141118145642-24928192-predictably-inaccurate-big-data-brokers/.
[19] MacMillan, *supra* note 18.

other data sets to predict and ultimately influence consumer behavior.[20] Consumers are largely unaware of how data brokers, the "fundamental actor of surveillance capitalism,"[21] shape their experience online "in ways that are entirely opaque to them."[22]

i. Data collection fuels data broker influence over consumers

Consumer browsing and purchasing habits are constantly monitored and tracked. There are myriad consequences from data brokers collecting, sharing, and selling these troves of consumer data. In addition to causing privacy and data security harms, data brokers use this data to influence consumer behavior.[23] The data can be packaged or analyzed to inform targeted advertising. As opposed to traditional advertising or contextual advertising, "data brokers simply access free data from individuals, who are generally unaware that their data is being repurposed and sold to third parties to convince users to purchase products they might not have otherwise bought."[24] The granular nature and massive scale of such data collection enables precise ad targeting and delivery to specific categories of people.[25] In this way, data brokers commodify user behavior: "their activity on the web is unconscious work for the benefit of internet companies."[26]

Although the rise of targeted advertising has only been possible with expansive data collection practices, data collection alone does not necessarily influence consumer purchasing patterns. The profiles that allow companies to target and shape consumer behavior are in large part

[20] *See* Urbano Reviglio, *The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview*, 11 Internet Pol'y Rev. 1, 2 (2022).
[21] *Id.*
[22] EPIC, Comments on FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 34, 87 Fed. Reg. 51273 (Nov. 21, 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter "EPIC Commercial Surveillance FTC Comments"].
[23] *Id.* at 34*; see also* Spandana Singh, New America, Special Delivery: How Internet Platforms Use Artificial Intelligence to Target and Deliver Ads 19 (2020), https://d1y8sb8igg2f8e.cloudfront.net/documents/Special_Delivery_FINAL_VSGyFpB.pdf.
[24] Reviglio, *supra* note 20, at 4.
[25] Singh, *supra* note 23, at 19.
[26] Reviglio, *supra* note 20, at 10.

the work of data brokers. Brokers amass, analyze and combine data sets from various sources to tailor their products and services to different types of customers, including advertisers.[27] This ecosystem "incentivizes rampant data collection as these systems require vast data sets in order to operate and improve."[28] The types of data that data brokers collect for consumer profiling can be extremely granular and sensitive. In addition to general interests or preferences, data collection can include financial data, health data, travel data, demographic information, location data, and more.[29] Moreover, privacy self-management is virtually impossible in view of the countless pathways through which brokers obtain data, including direct collection from individuals, cookies, software development kits (SDKs), third parties, web scraping, and other public records.[30] As data brokers constantly collect and package personal data into detailed profiles, there is "little consumer control over what information is being manipulated for corporate gain."[31]

When data brokers acquire, analyze and share detailed and specific information about consumers, they do so largely behind the scenes without any consumer knowledge or understanding.[32] Given this general lack of transparency and accountability, American consumers "neither understand commercial surveillance practices and policies nor feel they are capable of doing

[27] *Id.* at 5 ("The information, services and inferences they supply play central roles in key life decisions across a growing range of areas: a) advertising and marketing (e.g., micro-targeting or dynamic pricing), b) credit and insurance (e.g., for risk-mitigation), c) identity verification and fraud detection (e.g., credit bureaus or people-search sites), d) education, e) government and law enforcement and f) customer services.").
[28] Singh, *supra* note 23, at 19.
[29] *Id.; see also* 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.
[30] *See* Reviglio, *supra* note 20, at 5–6.
[31] Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 Wake Forest L. Rev. 433, 440 (2014).
[32] FTC, Data Brokers: A Call for Transparency and Accountability vii (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter "FTC Data Brokers Report"].

anything about rampant data extraction."[33] Even where consumers may be curious to investigate how their data is collected, processed, and sold, data brokers deploy tactics like placation, misnaming, diversion, or using obtuse jargon to overwhelm and contribute to "a feeling of resignation among consumers."[34]

ii. Consumers lack autonomy and choice

Consumers are largely unaware and powerless when it comes to the influence of data brokers over their purchasing patterns. Data brokers weaken consumer autonomy, as "[c]ommercial surveillance entities surreptitiously monitor consumers' browsing and purchasing habits, then use them to infer sensitive personal characteristics and modify consumer behavior."[35] Data brokers thwart consumer expectations about how their data is being collected and used online, and users have little recourse or ability to opt out of information collection.[36] Because consumers don't know how companies and data brokers are collecting and using their information, they are unable to correct, delete or access any information that was shared or collected about them online. In this way, data brokers have *greater* control over consumer data, behavior, and characteristics online than the consumer.[37] Not only do data brokers consistently and imperceptibly invade consumer privacy, but their efforts to aggregate, analyze, consolidate, and sell consumer data ultimately weaken consumer autonomy and choice.[38]

[33] Joseph Turow et al., Annenberg Sch. Commc'ns, U. Penn., Americans Can't Consent to Companies' Use of Their Data 17 (2023), https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf [hereinafter "Annenberg Report"].
[34] Knowledge at Wharton Staff, *Your Data is Shared and Sold . . . What's Being Done About It?*, Knowledge at Wharton (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/.
[35] EPIC Commercial Surveillance FTC Comments at 43.
[36] *See* Sophie Bushwick, "*Anonymous" Data Won't Protect Your Identity*, Sci. Am. (July 23, 2019), https://www.scientificamerican.com/article/anonymous-data-wont-protect-your-identity/.
[37] Tsesis, *supra* note 31, at 437.
[38] Reviglio, *supra* note 20, at 2.

Data brokers regularly deprive consumers of their ability to make their own choices online in a way that is largely invisible. Consumers are "subject to decisions made about them on the basis of personal data used as proxies and over which they might not have control."[39] Data brokers can also exploit the collective nature of such voluminous data analysis, as one individual's profile can reveal information about another person whose data indicates similar characteristics,[40] ultimately limiting the ability to remain anonymous online.[41] Even where a consumer *is* aware of the granular surveillance of their every click and scroll, that recognition may influence or restrict their ability to exercise free choice.[42]

Consumers are also subjected to discrimination and the loss of opportunity online. The profiles that data brokers amass, share, and sell to advertisers enable advertisers to precisely specify and target which categories of users to include or exclude from their marketing campaigns.[43] "While these determinations might result in some users receiving ads that are relevant to them, this can also result in the discriminatory exclusion of certain categories of users."[44] Moreover, the inclusion of automated tools in ad delivery can reinforce discriminatory prejudices and biases related to race, gender and socioeconomic status.[45] These forms of discrimination can lead to a loss of opportunity with harmful impacts online and offline because many industries advertising financial products,

[39] Inge Graef et al., *Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice*, 2 Digit. Soc'y 1, 19 (2023) ("Indeed, it is fundamental to take into account the individuals' capacity for not doing or wanting everything which they are "statistically" predisposed to do or want, and to always assert their right to themselves to account for their own motivations").
[40] *Id*.
[41] *See* Sheri B. Pan, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 Harv. J. L. & Tech. 240, 256 (2016).
[42] *Id*. at 254.
[43] Sherman, *supra* note 17, at 11.
[44] Singh, *supra* note 23, at 19.
[45] *Id*.

insurance, healthcare, employment or other opportunities purchase and use data brokers to target and regulate access to their services.[46]

An inability to correct or identify the use of consumer information can also lead to a loss of opportunity. For example, the mechanisms that inform scoring processes and other consumer analytics are not transparent to consumers. Consumers are automatically denied the ability to "mitigate the negative effects of lower scores, such as being limited to ads for subprime credit or receiving different levels of service from companies."[47] In the context of risk mitigation products, a consumer could be incorrectly flagged or denied the ability to conclude a transaction without recourse.[48] The inability to correct, control, manage or identify how data is being collected and used could contribute to consumer distrust in the marketplace.

iii. Data brokers play a central role in consumer purchasing patterns

One central role of data brokers within the broader commercial surveillance ecosystem is to influence purchasing patterns. Even data brokers that do not have direct relationships with consumers contribute to profiles that shape and influence consumer purchasing patterns and decisions online.[49] Data brokers commodify consumer behavior by predicting how consumers may act in the future, "and constructing mechanisms to influence these future behaviors, whether such behaviors are voting or making purchases."[50] In order to maintain their influence over consumer choice, the digital targeted advertising lifecycle requires and incentivizes tracking and constant data collection to operate and improve datasets.[51] Widespread data collection generally fuels targeted

[46] Sherman, *supra* note 43, at 9–10.
[47] FTC Data Brokers Report at 48.
[48] *Id.*; *see also* Tsesis, *supra* note 31, at 436 ("Lack of transparency about how companies, especially data brokers, transact in customer information often limits consumers' control over data in ways that cause significant harms to reputation and privacy.").
[49] EPIC Commercial Surveillance FTC Comments, *supra* note 22, at 34.
[50] Singh, *supra* note 23, at 19.
[51] *Id.*

advertising, and data brokers are relied on as middle actor to effectively influence consumer purchasing patterns.

f. The false promise of deidentification

The following is responsive to Question 10.

Consumer data can often be readily reidentified from a deidentified data set. Although data brokers strive to assuage consumers and regulators by broadcasting that the data they sell is anonymized, "the theory that data scrubbed of personally identifying information cannot be re-identified has time and again been shown to no longer hold true."[52] There are many reidentification methods that can be used individually or in tandem to reidentify data, like insufficient deidentification, aggregation or combining data sets.[53] Even incomplete data sets can be easily reidentified at a highly accurate level, identifying precise information about individuals based on various patterns and characteristics.[54] A 2019 study published in Nature found that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes."[55]

The ability to reidentify anonymized or scrubbed data sets is widely known and central to the data broker business model. For example, the Census Bureau now uses differential privacy methods to guard against efforts to reidentify Census participants.[56] Even when a data set is scrubbed of personal information, the data broker or purchaser "likely [has] access to sufficient information that

[52] Boris Lubarsky, *Re-Identification of Anonymized Data*, 1 Geo. L. Tech. Rev. 202, 213 (2017).
[53] *Id*. at 208–11.
[54] *See* Cameron F. Kerry & Mishaela Robison, *Rulemaking In Privacy Legislation Can Help Dial In Ad Regulation*, Brookings Inst. (Dec. 5, 2022), https://www.brookings.edu/blog/techtank/2022/12/05/rulemaking-in-privacy-legislation-can-help-dial-in-ad-regulation/.
[55] Luc Rocher et al., *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, 10 Nature Commc'ns 1, 2 (2019).
[56] Mike Schneider, *Census Bureau Chief Defends New Privacy Tool Against Critics*, Associated Press (Nov. 28, 2022), https://apnews.com/article/technology-census-2020-us-bureau-censuses-government-and-politics-e007a75ba167659138a8648e1e98133b.

their systems can be used to re-identify or link data to individuals across data sets."[57] Data brokers and similar companies regularly provide sophisticated re-identification techniques for cross-device tracking and merging data sets, often using machine learning to analyze massive amounts of data.[58]

Anonymization and transparency are in many ways incompatible today's data broker business models.[59] Relying on sustained information asymmetry, consumers are necessarily kept in the dark with no ability to opt out of data collection and aggregation.[60] This unrestrained and largely unregulated surveillance and aggregation enables data brokers to provide detailed analytics to their customers. While one data point may not be helpful for targeted advertising, "millions and millions of data points allow data brokers to link information to individual consumers."[61]

III. The Negative Impacts of Ubiquitous Commercial Data Collection on Consumers

Every year, data-extractive products and services collect granular information about millions of consumers, providing data brokers with data worth over $185 billion.[62] These products and services collect consumers' personal data in several different ways during the course of their routine online and offline activities: by loading content from a website, app, service, or connected device; interacting with these websites, apps, services, and connected devices; and even walking through stores and neighborhoods that track people through sensors and surveillance devices, consumers knowingly and unknowingly provide data brokers with extremely granular data about who they are, where they go, and what they like.[63]

---

[57] EPIC Commercial Surveillance FTC Comments at 43 (citing Lubarsky, *supra* note 52; Danny Bradbury, *De-identify, Re-identify: Anonymised Data's Dirty Little Secret*, Register (Sept. 16, 2021), https://www.theregister.com/2021/09/16/anonymising_data_feature/.)
[58] Reviglio, *supra* note 24, at 13.
[59] *Id*.
[60] *See id*. ("Privacy asymmetry is indeed a cornerstone of the data broker business model.").
[61] EPIC Commercial Surveillance FTC Comments at 39–40.
[62] José Bayoán Santiago Calderón & Dylan G. Rassier, *Valuing the U.S. Data Economy Using Machine Learning and Online Job Postings* 26 (U.S. Bureau Econ. Analysis, Working Paper No. 2022-13, 2022), https://www.bea.gov/system/files/papers/BEA-WP2022-13.pdf.
[63] *See* FTC Data Brokers Report at iv; EPIC Commercial Surveillance FTC Comments at 35–36.

This section of EPIC's comment highlights the experiences of these millions of consumers. It details how ubiquitous and unavoidable data collection undermines consumers' privacy, autonomy, and control over their data; how data brokers extract value from consumers largely without their knowledge; and how voracious data collection and use can harm even those consumers who have taken steps to keep their data private and secure. Far from being active, equal participants in the data market, countless consumers are surveilled and exploited for their data in ways that produce consumer harms and undermine competition within data-centric markets.

a. The unavoidability of the data trade

The following is responsive to Question 9 and 15.

Data collection is unavoidable, leaving consumers without meaningful control over the collection, use, resale, and sharing of their data. From the moment a child is born—and sometimes even before[64]—their life is tracked, digitized, and commodified.[65] Their name, birthdate, and place of birth, as well as the names, addresses, birthdates, and occupations of their parents, are collected in birth certificates and other public records that data brokers buy in droves.[66] Their health data is collected and compiled through connected devices and child-rearing apps[67] or bought commercially

[64] *See, e.g.*, Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info on Pregnant People*, Politico (Aug. 1, 2022), https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988; Shoshana Wodinsky & Kyle Barr, *These Companies Know When You're Pregnant—And They're Not Keeping it Secret*, Gizmodo (July 30, 2022), https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426.

[65] *See, e.g.*, Richard Godwin, *'You Can Track Everything': The Parents Who Digitise Their Babies' Lives*, Guardian (Mar. 2, 2019), https://www.theguardian.com/lifeandstyle/2019/mar/02/apps-that-track-babies-and-give-data-to-tech-firms-parents.

[66] *See* 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.

[67] *See* Godwin, *supra* note 65; Anna Werner, *Experts Warn Smart Toys for Children Could be Collecting User Data That Might be Sold*, CBS News (Dec. 29, 2022), https://www.cbsnews.com/news/smart-toys-data-collecting-advertisers/; Drew Harwell, *AI Baby Monitors Attract Anxious Parents: 'Fear is the Quickest Way to Get People's Attention*,' Wash. Post (Feb. 25, 2020), https://www.washingtonpost.com/technology/2020/02/25/ai-baby-monitors/ (detailing how smart baby monitors collect information about babies' faces and cries to further train their algorithms).

as health records.[68] At school, they are tracked by various educational technology ("edtech") tools[69] and surveilled by camera systems.[70] At home, the digital devices they use for work, entertainment, and social interaction hoover up their data at every step: websites and third-parties embed text files called "cookies" that surreptitiously collect and store their identifying information across countless websites;[71] the digital platforms they use compile detailed profiles about them based on their personal information, behavior, and inferences drawn from both;[72] and data brokers scrape information from what they post online.[73] Even when a child leaves their digital devices behind,

[68] *See, e.g.*, Drew Harwell, *Now for Sale: Data on Your Mental Health*, Wash. Post (Feb. 13, 2023), https://www.washingtonpost.com/technology/2023/02/13/mental-health-data-brokers/; Justin Sherman, *Your Health Data Might Be for Sale*, Slate (June 22, 2022), https://slate.com/technology/2022/06/health-data-brokers-privacy.html; Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Sci. Am. (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

[69] Hye Jung Han, Human Rights Watch, "How Dare They Peep into My Private Life?": Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic (2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments [hereinafter "Human Rights Watch Edtech Report"]; Drew Harwell, *Remote Learning Apps Shared Children's Data at a 'Dizzying Scale*,' Wash. Post (May 24, 2022), https://www.washingtonpost.com/technology/2022/05/24/remote-school-app-tracking-privacy/.

[70] *See* Katherine Schaeffer, *U.S. School Security Procedures Have Become More Widespread in Recent Years But Are Still Unevenly Adopted*, Pew Rsch. Ctr. (July 27, 2022), https://www.pewresearch.org/short-reads/2022/07/27/u-s-school-security-procedures-have-become-more-widespread-in-recent-years-but-are-still-unevenly-adopted/ ("The majority [of public schools] reported using security cameras to monitor the school (91%).").

[71] Dave Davies, *User's Beware: Apps are Using a Loophole in Privacy Law to Track Kids' Phones*, NPR (June 16, 2022), https://www.npr.org/2022/06/16/1105212701/users-beware-apps-are-using-a-loophole-in-privacy-law-to-track-kids-phones; Colin Lecher, *Who's Allowed to Track My Kids Online?*, Markup (Mar. 10, 2020), https://themarkup.org/the-breakdown/2020/03/10/websites-tracking-kids-coppa.

[72] 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; Grauer, *supra* note 66.

[73] *See* Marissa Newman, *Meta Was Scraping Sites for Years While Fighting the Practice*, Bloomberg (Feb. 2, 2023), https://www.bloomberg.com/news/articles/2023-02-02/meta-was-scraping-sites-for-years-while-fighting-the-practice; Emily Stewart, *Why Every Website Wants You to Accept Its Cookies*, Vox (Dec. 10, 2019), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy ("There are first-party cookies that are placed by the site you visit, and then there are third-party cookies, such as those placed by advertisers to see what you're interested in and in turn serve you ads—even when you leave the original site you visited. (This is how ads follow you around the internet.)"); *cf.* Melissa Heikkilä, *What Does GPT-3 "Know" About Me?*, MIT Tech. Rev. (Aug. 31, 2022), https://www.technologyreview.com/2022/08/31/1058800/what-does-gpt-3-know-about-me/ (discussing practice of training large language models by scraping social media data).

extensive networks of sensors and cameras collect information about them as they move throughout the physical world.[74]

As children grow up, the extent to which data-extractive technologies extract and exploit their data only increases. Common life events—buying a car, registering to vote, getting married, and opening a credit line—all produce new and more granular consumer data that data brokers buy and sell.[75] Everyday activities like purchasing groceries, watching television, and posting on social media produce data that data brokers compile into extensive accounts of who we are.[76] And even when someone tries to protect their data, many data-extractive technologies have become indispensable for modern life. Education, work, banking, checking one's voter registration, and so much more all rely on data-extractive tools and online services that force people to surrender their data for access.[77]

These examples highlight one inescapable truth: the average person cannot effectively avoid data collection, even if they want to. Extensive and persistent data collection is an integral part of the systems that enable consumers to browse websites, access online services, and interact with mobile applications.[78] And many of these online services are essential for consumers' livelihoods. In a 2021

[74] *See* FTC Data Brokers Report at iv; Julie Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 Phil. & Tech. 213, 219–20 (2017) (describing the "extension of surveillance capability" over time to capture personal and biometric information through sensing networks and facial recognition technology).
[75] *See* Sherman, *supra* note 43, at 4–8 (detailing what data several leading data brokers collect).
[76] *See, e.g.*, Jon Keegan, *Forget Milk and Eggs: Supermarkets are Having a Fire Sale on Data About You*, Markup (Feb. 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you; Hooman Mohajeri Moghaddam et al., *Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices*, Proc. 2019 ACM SIGSAC Conf. on Comput. & Commc'ns Sec. 131 (Nov. 6, 2019), https://dl.acm.org/doi/pdf/10.1145/3319535.3354198; Newman, *supra* note 73.
[77] *See, e.g.*, U.S. Gov't Accountability Off., *Why Do Banks Share Your Financial Information and Are They Allowed To?*, GAO WatchBlog (Dec. 9, 2020), https://www.gao.gov/blog/why-do-banks-share-your-financial-information-and-are-they-allowed.
[78] EPIC Commercial Surveillance FTC Comments at 55.

Pew Research Center survey, 90% of consumers said that the internet was "essential or important,"[79] and the average consumer spends nearly seven hours a day online.[80] Increasingly, these data-extractive websites, online services, and mobile applications are following consumers throughout their daily lives as well: in 2021, 85% of Americans owned a smartphone or similar connected device, up from 35% in 2011.[81] These devices not only extend the reach of data-extractive online services, but also impose new forms of data collection and use on consumers, including facial recognition[82] and geolocation tracking.[83]

Three demographics—low-income populations, children, and migrants—are especially vulnerable to modern data collection practices. First, consider low-income populations. To cover expenses and feed their families, many low-income individuals rely on public benefits, short-term loans, and other cash assistance services that force them to provide extensive personal data in exchange for assistance. Many of these assistance programs not only collect data about low-income individuals, but also share it with data brokers. For example, several state unemployment agencies contract with large data brokers like Thomson Reuters and Deloitte conduct screening for benefits fraud, wherein each vendor matches a benefits applicant's information to consumer profiles within their extensive database of user information to flag discrepancies.[84] Many predatory private lending

[79] Colleen McClain et al., *The Internet and the Pandemic*, Pew Rsch. Ctr. (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/.
[80] Simon Kemp, *Digital 2021 April Global Statshot Report*, Data Reportal (Apr. 21, 2021), https://datareportal.com/reports/digital-2021-april-global-statshot.
[81] *Mobile Fact Sheet*, Pew Rsch. Ctr. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.
[82] *See* U.S. Gov't Accountability Off., GAO-20-522, Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses 10 (2020), https://www.gao.gov/products/gao-20-522.
[83] *See* Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data; Thompson & Warzel, *supra* note 29.
[84] *See* EPIC, Screened & Scored in the District of Columbia 24 (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf [hereinafter "EPIC Screened & Scored Report"]; *EPIC Screening and Scoring Spotlight: Pondera's Fraud Prediction Algorithms for Public Benefits*, EPIC, https://epic.org/pondera-surveillance/ (last visited July 11, 2023).

services use consumer data to deliberately seek out "financially vulnerable borrowers for deceptive sales tactics"—a practice sometimes called "reverse redlining."[85] And for their part, many major data brokers specifically target low-income populations, grouping consumer data into marketing lists with titles like "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Retiring on Empty: Singles," "Tough Start: Young Single Parents," and "Credit Crunched: City Families."[86]

For low-income populations—a disproportionate percentage of whom are from racial or ethnic minority backgrounds[87]—data collection and targeting are inescapable. Data-extractive and predatory service providers, many of whom contract with government agencies to operate crucial public benefits programs, force low-income individuals into what Virginia Eubanks, author of *Automating Inequality*, calls the "digital poorhouse": the very data that low-income populations provide agencies and private lenders is used to invalidate their eligibility for public benefits and direct predatory lending services, reinforcing low-income populations' dependency on data-extractive assistance programs.[88]

Next, consider children. Any information asymmetry that exists between data-extractive companies and adult consumers is exacerbated when children and teens are subjected to data

[85] *Id.* at 6; *see also* Linda E. Fisher, *Target Marketing of Subprime Loans: Racialized Consumer Fraud and Reverse Redlining*, 18 J. L. & Pol'y 122 (2009); James A. Allen, *The Color of Algorithms: Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 Fordham Urb. L.J. 219 (2019).
[86] U.S. Senate Comm. on Com., Sci., & Transp., A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes (2013), https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577. [hereinafter "Senate Data Broker Report"].
[87] *See* John Creamer, *Inequalities Persist Despite Decline in Poverty For All Major Race and Hispanic Origin Groups*, U.S. Census Bureau (Sept. 15, 2020), https://www.census.gov/library/stories/2020/09/poverty-rates-for-blacks-and-hispanics-reached-historic-lows-in-2019.html; Vanessa Williamson, *Closing the Racial Wealth Gap Requires Heavy, Progressive Taxation of Wealth*, Brookings Inst. (Dec. 9, 2020), https://www.brookings.edu/research/closing-the-racial-wealth-gap-requires-heavy-progressive-taxation-of-wealth/.
[88] *See* Adele Peters, *Algorithms are Creating a "Digital Poorhouse" that Makes Inequality Worse*, Fast Co. (Mar. 1, 2018); *see generally* Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).

collection. The primary driver of this informational asymmetry is that data collection practices are non-obvious to consumers: the technical methods that online services and data brokers use to track consumers across services and devices, as well as the consumer profiles that companies create based on user data, are hidden from consumers' view. Because children and teens are still developing critical thinking skills, many children and teens find it more difficult than adults to identify when their data is being collected or when they are being targeted for advertisements.[89] And because many minors do not know how and when they are tracked online, they have no way to avoid being tracked.[90] UNICEF came to a similar conclusion in 2021: calling for greater data protections for children, UNICEF found that minors are not only more vulnerable consumers than adults, but also less likely to appreciate the longer-term repercussions of commercial data collection.[91] Despite legal safeguards on minors' personal data like the Children's Online Privacy Protection Act (COPPA),[92] commercial surveillance of minors persists at an expansive scale.[93] One recent study found that 67% of apps used by preschool-aged children collected persisted digital identifiers and transmitted them to third-party companies.[94] Many of these apps were "child directed" and likely in violation of

[89] *See* Ofcom, Children and Parents: Media Use and Attitudes Report 12–13 (2017), https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf.
[90] *See* Duncan McCann, New Econ. Found., I-Spy: The Billion Dollar Business of Surveillance Advertising to Kids 16 (2021), https://neweconomics.org/uploads/files/i-Spy__NEF.pdf.
[91] UNICEF, The Case for Better Governance of Children's Data: A Manifesto 2–5 (2021), https://www.unicef.org/globalinsight/media/1771/file/UNICEF%20Global%20Insight%20Data%20Governance%20Summary.pdf.
[92] 15 U.S.C. §§ 6501–06.
[93] *See, e.g.*, Geoffrey A. Fowler, *Your Kids' Apps are Spying on Them*, Wash. Post (June 9, 2022), https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy/ ("More than two-thirds of the 1,000 more popular iPhone apps likely to be used by children collect and send their personal information to the advertising industry[.] On Android, 79 percent of popular kids apps do the same."); Pixalate, Mobile Apps: Google v. Apple COPPA Scorecard (Children's Privacy) (2022), https://www.pixalate.com/hubfs/Reports_and_Documents/Mobile%20Reports/2022/App%20Reports/Active%20Apps/Child-Directed%20Apps/Q1%202022%20-%20Apple%20vs.%20Google%20COPPA%20Scorecard%20Report%20-%20Pixalate.pdf.
[94] Fangwei Zhao et al., *Data Collection Practices of Mobile Applications Played by Preschool-Aged Children*, JAMA Pediatrics, 2020, at 4, https://jamanetwork.com/journals/jamapediatrics/fullarticle/2769689.

COPPA,[95] while in other cases COPPA did not apply because the preschooler was using a general audience app.[96]

The rise of data-extractive edtech tools exacerbates the privacy challenges facing children.[97] Many children are exposed to data-extractive edtech tools without their parents' knowledge, and even when parents are given advance notice about edtech tools, many parents lack the time and technical knowledge necessary to adequately evaluate edtech tools and make informed choices about their children's privacy. When these tools are mandatory aspects of homework, test taking, school communication, or the storage of educational files, even families who want to avoid data collection are left without meaningful choice. During the COVID-19 pandemic, what little choice families had about their children's privacy shrank further.[98] One analysis demonstrated that 89% of edtech products endorsed by the governments of 49 countries during the COVID-19 pandemic either "put at risk or directly violated children's privacy and other children's rights[] for purposes unrelated to their education."[99] Many of these tools—112 of 164 analyzed—included several embedded third-party trackers, meaning that, just by logging into these edtech tools, minors were being tracked by an average of six third-party data collectors per day.[100]

Migrants and refugees coming to the United States are also at particularly high risk for data abuse. These populations risk direct harms if their personal data is obtained by agencies like the

[95] *Id.* at 2 ("Binns and colleagues used static app analysis (i.e., analyzing app source code to find code that directs data collection to third parties) on 959,000 apps from the US and UK Google Play stores. They found that apps targeting children had among the highest number of third-party trackers. Reyes et al. used dynamic analysis to track the data transmissions from 5855 of the most popular free Android children's apps and showed that the majority had potential COPPA violations.").
[96] *Id.* at 6 ("[S]ome children in our study used apps that transmit geolocation data, such as the McDonald's app, and games such as hole.io and SpeedBall. Children may easily download general audience apps from Google Play when parental controls are not enabled. It is also possible that children install adult-directed apps through advertisements that appear in children's apps, where they can easily be clicked and installed.").
[97] *See* Human Rights Watch Edtech Report, *supra* note 69.
[98] *See id.*
[99] *Id.*
[100] *Id.*

Department of Homeland Security. Undocumented immigrants face the most acute risk—deportation—but even documented migrants and refugees risk increased surveillance, profiling, raids, and other abuse from immigration officials.[101] Many of these programs are run by major data brokers like LexisNexis, which contracts with federal agencies like the U.S. Immigration and Customs Enforcement (ICE) to provide detailed information and analytics about migrant communities.[102] And the use of commercial data about migrants runs deep: in 2021, for example, over 11,000 ICE officials used LexisNexis data and predictive analytics services to screen and vet immigrants, analyze potential criminal risks, and pursue deportation enforcement actions.[103] Ubiquitous commercial data collection not only violates the privacy of vulnerable groups like migrants, but also facilitates physical and economic harms by both commercial and government actors.

Modern data collection is both ubiquitous and invisible. Current trends in the data trade have left consumers unable to meaningfully control their data, unable to consent to data collection, unable to escape data collection, and even unable to understand when and how data collection occurs. Despite how commonplace data collection is today, a 2022 study by NORC at the University of Chicago found that only 71% of consumers knew that online companies were collecting their data, and only about half knew specific information about how those companies could track them.[104] A 2019 Pew Research study found similar results: 78% of Americans did not understand what the

[101] *See, e.g.*, Sam Biddle, *LexisNexis Is Selling Your Personal Data to ICE So It Can Try to Predict Crimes*, Intercept (June 20, 2023), https://theintercept.com/2023/06/20/lexisnexis-ice-surveillance-license-plates/; Johana Bhuiyan, *A US Surveillance Program Tracks Nearly 200,000 Immigrants. What Happens to Their Data?*, Guardian (Mar. 14, 2022), https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap.
[102] Biddle, *supra* note 101. Note, however, that federal agencies are buying swaths of commercial consumer data about citizens without warrants as well. *See, e.g.*, Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, Brennan Ctr. for Just. (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.
[103] *Id.*
[104] Annenberg Report at 10.

government does with their data, and 59% did not understand how data companies use their data.[105] Consumer ignorance of data collection practices is no coincidence: several companies have intentionally used surreptitious data collection and processing to profit off user data without disclosing secondary uses and sales.[106] With data collection hidden from view, many consumers have no reason to anticipate that their data may be collected or misused, let alone take steps to avoid it.[107]

Even when consumers are generally aware of data collection, most do not know what they can and cannot do to control their data.[108] Often this confusion is by design: many companies providing data-extractive products and services actively obfuscate the ways they collect and use consumer data through default options,[109] dark patterns,[110] and abstruse privacy policies.[111] These obfuscation practices make it incredibly difficult for consumers to control their data online, even if they want to. For example, many websites now require consumers to provide their mobile phone number in order to create an account or access a product.[112] These phone numbers—sometimes

---

[105] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ ("But even as the public expresses worry about various aspects of their digital privacy, many Americans acknowledge that they are not always diligent about paying attention to the privacy policies and terms of service they regularly encounter.").

[106] EPIC Commercial Surveillance FTC Comments at 155–56. The FTC has recently pursued administrative actions against companies who collect and use consumer data for undisclosed purposes. *See, e.g.*, *In re Support King, LLC (SpyFone.com)*, FTC File No. 192-3003 (2021); *In re Sears Holdings Mgmt. Corp.*, FTC File No. 082-3099 (2018); *In re Lenovo*, FTC File No. 152-3134 (2018); *In re Twitter*, FTC File No. 202-30623 (2022).

[107] EPIC Commercial Surveillance FTC Comments at 157; *see also IFC Credit Corp.*, 543 F. Supp. 2d at 948; *Orkin Exterminating Co.*, 849 F.2d at 1365 ("[C]onsumers may act to avoid injury before it occurs *if they have reason to anticipate the impending harm and the means to avoid it*[.]") (emphasis added).

[108] Annenberg Report at 10.

[109] *See, e.g.*, Brian X. Chen, *The Default Tech Settings You Should Turn Off Right Away*, N.Y. Times (July 27, 2022), https://www.nytimes.com/2022/07/27/technology/personaltech/default-settings-turn-off.html.

[110] *See* FTC, *Bringing Dark Patterns to Light* 1–2, 15–19 (2022), https://www.ftc.gov/reports/bringing-dark-patterns-light [hereinafter "FTC Dark Patterns Report"].

[111] *See, e.g.*, Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. Times (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[112] FTC Dark Patterns Report at 16.

likened to Social Security numbers because consumers rarely, if ever, change them—are then sold to data brokers and used by data-extractive companies to identify consumers for targeted advertising.[113] Similarly, products like Google's Android phone enables location data sharing by default when consumers set up the phone, often giving Google access to consumers' granular location data without their knowledge or consent.[114]

Together, the ubiquity of data-extractive technologies and the active steps that data-extractive companies and data brokers take to obfuscate their data collection practices make it impossible for the average consumer to avoid having their information collected, processed, used, and sold.

b. The consumer harms of the data trade

The following is responsive to Questions 11, 13, and 16.

Data broker practices can harm consumers both directly and indirectly, affecting even those who have attempted to avoid data collection. These harms stem not only from consumer perceptions about the possibility of misuse and harm, but also from the real harms that unconstrained data collection and use impose on consumers every day. These harms vary widely across populations and use contexts, but generally fall into two categories: (1) direct consumer privacy harms and (2) indirect consumers harms that result from abusive secondary uses and other adverse consequences of data collection.

The direct consumer privacy harms that result from data collection and misuse are real and legally cognizable.[115] However, many regulators and courts fail to recognize when and to what extent direct privacy harms occur. Unlike many other forms of consumer harm, data privacy harms tend to be small but numerous, meaning that a consumer may be harmed similarly and frequently in small

[113] *Id.*; *see also* Complaint for Permanent Injunction and Other Relief, *FTC v. Kochava, Inc.*, 2:22-cv-00377-DCN, 9 (D. Idaho filed Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
[114] FTC Dark Patterns Report at 16.
[115] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 799–815 (2022).

ways when data brokers use, sell, or process their data.[116] Additionally, consumers may not immediately feel the harms that result from data broker practices, making it difficult for them to know the severity of their harm until much later. Consider, for example, the consumer harms that result from a data breach, such as economic harms resulting from identity theft or fraud.[117] Major data brokers compile extensive data profiles of millions of consumers, but when their databases are breached, consumers may not immediately feel the full repercussions of the breach; injuries that result from harms like identity theft or fraud are often delayed since malicious actors may not immediately attempt to use the breached consumer data.[118] In fact, consumers may never be able to trace data privacy harms to any one data breach either; by the time they experience a data privacy harm, their data may have passed between numerous third-parties, all of whom may have acquired the data from multiple sources.[119] Additionally, different malicious actors may use breached data for different purposes at different times, resulting in a series of separate injuries spanning several months or years.

Direct consumer privacy harms go beyond economic harms as well; they encompass everything from physical harms to reputational harms, psychological harms, autonomy harms, discrimination harms, and relationship harms.[120] "Many [of these consumer] privacy violations involve broken promises or thwarted expectations about how people's data will be collected, used,

[116] *Id.* at 816.
[117] *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737, 747–67 (2018). Recent research by Incogni suggests that 26 data brokers have experienced data breaches since 2002, impacting over half a billion consumers. Federico Morelli, *Are US Data Brokers Able to Protect the Personal Information They Deal In?*, Incogni Blog (Feb. 18, 2023), https://blog.incogni.com/data-brokers-breaches/.
[118] Solove & Citron, *supra* note 117, at 750.
[119] *Cf.* Solove & Citron, *supra* note 117, at 775–76.
[120] *See generally* Citron & Solove, *supra* note 115.

and disclosed."[121] And just like with data breach harms, some of these violations may "appear small when viewed in isolation, such as the inconvenience of receiving an unwanted email or advertisement or the failure to honor people's expectations that their data will not be shared with third parties. But when done by hundreds or thousands of companies, the harms add up…. [T]hese harms are dispersed among millions—and sometimes billions—of people and can be hard to combat absent [agency] intervention."[122] The extent of these direct privacy harms can depend on "how the data is used, what data is involved, and how the data might be combined with other data. Sharing an innocuous piece of data with another company might provide a key link to other data or allow for certain inferences to be made," which can extend the downstream impacts of data sharing.[123] For example, information concerning someone's age, gender, location, or search history may seem relatively innocuous when shared separately, but when the information is combined, it can and has been used to identify and harass individuals seeking sensitive services like abortions[124] or out gay clergymen without their consent.[125]

The large-scale collection and resale of consumer data can also lead to more immediate and visceral privacy harms. For example, many data brokers offer "people search" services, whereby an individual consumer can purchase granular information about another's background, location, and

[121] *Id.* at 797 (citing Jacqueline D. Lipton, *Mapping Online Privacy*, 104 N.W. U. L. Rev. 477, 508 (2010) (noting "the greatest harms in the present age often come from unauthorized uses of private information online," including the improper collection, aggregation, processing, and dissemination of information)).
[122] *Id.* at 797 (citing Brian Fung, *T-Mobile Says Data Breach Affects More than 40 Million People*, CNN Business (Aug. 18, 2021), https://www.cnn.com/2021/08/18/tech/t-mobile-data-breach/index.html.).
[123] *Id.* at 818.
[124] *See* Sara Geoghegan & Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC Blog (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/.
[125] *See* Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data that Tracked Gay Priests*, Wash. Post (Mar. 9, 2023), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/.

affiliations.[126] Unlike data broker practices aimed at corporate marketing, people search websites are directed toward individuals, who may use the data they purchase to "track[] the activities of executives and competitors, find[] old friends, research[] a potential love interest or neighbor, network[], or locat[e] court records."[127] While some of these people search websites only sell information derived from public sources like property records, others sell information derived or inferred from private and commercial databases.[128] Worse still, many people search websites do not verify the accuracy of consumer data they receive, sometimes conflating data from multiple consumers or incorporating other inaccurate information into consumer profiles that they then sell to other consumers or data brokers.[129] And the proliferation of people search websites implicates physical, autonomy, and reputational privacy harms in direct and significant ways as well: the data that brokers sell to individuals through these websites can be used to stalk and harass individuals[130] or undermine a consumer's relationships and access to professional opportunities.[131] At worst, people search websites facilitate physical harm. As far back as 2003, for example, the people search

[126] *See What to Know About People Search Sites That Sell Your Information*, FTC (July 2022), https://consumer.ftc.gov/articles/what-know-about-people-search-sites-sell-your-information; Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 Y. J. on Reg. 667, 675–76 (2017).
[127] FTC Data Brokers Report at 34.
[128] Rostow, *supra* note 126, at 675; U.S. Gov't Accountability Off., GAO-13-663, Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace 3–4 (2013) (noting that many U.S. brokers offer people search services that incorporate data from "proprietary sources").
[129] *See* Dell Cameron, *How the US Can Stop Data Brokers' Worst Practices—Right Now*, Wired (Feb. 8, 2023), https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/; Levi Kaplan et al., *Measuring Biases in a Data Broker's Coverage*, 2017 AMC IMC Conf. Proc. 3–6, https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Kaplan-Mislove-Sapiezynski-Measuring-Biases-in-a-Data-Brokers-Coverage.pdf.
[130] *See* Adi Robertson, *Senators Ask FTC to Fight Stalkers Exploiting People Search Sites*, Verge (Mar. 4, 2021), https://www.theverge.com/2021/3/4/22313613/ftc-senator-letter-stalking-abuse-data-broker-people-search-sites.
[131] *See* Rostow, *supra* note 126, at 672; Citron & Solove, *supra* note 115, at 849–60; Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 Berkeley Tech. L.J. 2073, 2091–93 (2015) (describing the privacy interest in avoiding social sorting, which involves "obtain[ing] personal and group data in order to classify people and populations according to varying criteria" and discrimination); Margaret Hu, *Big Data Blacklisting*, 67 Fla. L. Rev. 1735 (2015).

website, Docusearch, sold a New Hampshire woman's location data to one of her acquaintances, who then used that data to stalk, harass, and ultimately murder her.[132]

Direct consumer privacy harms can also extend to individuals who take active steps to protect their data from collection. Data brokers do not restrict their databases to data collected directly from individuals; many include data inferences derived from connections between different databases or information provided by other companies and users.[133] For example, a data broker may combine data purchased from different social media platforms together based on matching names and email addresses within different consumer data profiles, or they may infer information about a consumer based on the presence of proxy variables, which may provide more information about a consumer's demographic profile when placed within historical context. ZIP codes, for example, may be proxy variables for race and socioeconomic status given the United States' long history of redlining.[134] Data brokers may also build "shadow profiles" of consumers whose data profiles are missing or incomplete based on the information provided by other consumers. For example, when a user joins Facebook and permits Facebook to access her phone contacts, Facebook may create shadow profiles of people in the user's contact list who do not have a Facebook account.[135] These profiles serve as simulacra of Facebook user data profiles: they may include mutual connections between several users who all have the shadow profile's contact information, or they may reflect data about the non-user that Facebook has purchased from a data broker. In either case, Facebook

[132] *See Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1006 (N.H. 2003).
[133] EPIC Commercial Surveillance FTC Comments at 27; *see also* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2 Colum. Bus. L. Rev. 494 (2019).
[134] EPIC Screened & Scored Report at 23; *see also* Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1257 (2020); Devin G. Pope & Justin R. Sydnor, *Implementing Anti-Discrimination Policies in Statistical Profiling Models*, 3 A. Econ. J. 206, 209 (2011).
[135] *See, e.g.*, Andrew Quodling, *Shadow Profiles–Facebook Knows About You, Even If You're Not on Facebook*, Conversation (Apr. 13, 2018), https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804.

has created a data profile about a consumer who has refrained from joining the platform, and Facebook may use the consumer's data in ways that produce privacy harms even without the consumer's consent or presence on the platform.

The practices of compiling "shadow profiles" about consumers through data inferences and reselling consumer profiles to other data brokers and consumers make it difficult for any individual to avoid the adverse consequences of the data trade. With over 4,000 data brokers and countless other data-reliant companies popping up every day,[136] it can be incredibly difficult—if not impossible—for any one consumer to scrub their information from the internet. The same is true for consumers trying to correct inaccurate data once it has entered the data trade. One consumer's data may be shared, sold, processed, repackaged, and resold numerous times by numerous different data brokers, all of whom may have complex processes for requesting the removal or correction of consumer data.[137] For example, consumers may need to provide proof of identity, send a physical opt-out letter, or send in their request for data correction or deletion via fax machine.[138] Worse still, because many data brokers regularly repurchase or reshare consumer databases, consumers will often need to repeat the same opt-out process for each data broker multiple times a year in order to meaningfully control their data.[139]

Inaccurate data inferences made by data brokers can concretely impact consumers' lives as well. Consider the use of consumer databases for tenant screening services. The D.C. Housing Authority, for example, partners with a third-party vendor, RentGrow, to screen applications for its

[136] *See* Laura Martisiute, *Data Brokers: Your Comprehensive Guide*, DeleteMe (Feb. 3, 2023), https://joindeleteme.com/blog/what-are-data-brokers/.
[137] *See* Yael Grauer, *How to Delete Your Information from People-Search Sites*, Consumer Reps. (Aug. 20, 2020), https://www.consumerreports.org/personal-information/how-to-delete-your-information-from-people-search-sites-a6926856917/.
[138] *Id.*
[139] *Id.*

Housing Choice Voucher program.[140] To screen applicants, RentGrow generates a report connecting an individual's application to likely matches within commercial databases compiled by data brokers; it uses data like past eviction information, credit scores, and social media profiles to make recommendations of whom the government agency should accept into its housing voucher program.[141] If the report includes inaccurate information about an applicant (e.g., inaccurate data inferences or data from another person with a similar name), the applicant may be incorrectly denied housing.[142] If an applicant believes the information RentGrow has compiled is inaccurate, they can contest RentGrow's report directly, but the inaccuracies do not disappear from other commercial databases—and when RentGrow and similar companies purchase updated data from data brokers, these inaccuracies can return to even databases that consumers have taken steps to correct. In other words, any steps that a consumer takes to control or delete their data are nondurable; they require a consumer to vigilantly monitor commercial databases to exercise even moderate control over their data.

Many data broker practices can also fuel indirect consumer harms by providing data used to train and maintain harmful automated decision-making systems. Commercial entities and government agencies alike use automated decision-making systems for a broad range of purposes, including everything from simple statistical evaluation to sophisticated machine-learning applications. All of these purposes require automated decision-making systems to use and be trained on data. Some sophisticated machine-learning models like OpenAI's ChatGPT directly scrape information—including consumer data—from across the internet,[143] while many automated

[140] Contract between D.C. Housing Authority and RentGrow, Inc. (2018), https://perma.cc/QDD7-QHXM; *see also* EPIC Screened & Scored Report at 23, 25.
[141] *Id.*
[142] *See* EPIC Screened & Scored Report at 9, 27, 48 n.22.
[143] *See* Kevin Schaul et al., *Inside the Secret List of Websites that Make AI Like ChatGPT Sound Smart*, Wash. Post (Apr. 19, 2023), https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/.

decision-making systems are trained using commercial datasets derived from information compiled by data brokers.[144] Regardless of how the developers of these systems acquire consumer data, the result is the same: without consumers' knowledge or consent, their data can be collected and used to train a wide variety of automated decision-making systems that can negatively impact the public. The consumer would not profit off the use of their data to create or improve these systems—and they would have no choice in the matter.

Like commercial data collection, automated decision-making systems trained on consumer data are unavoidable. They are used throughout the economy, from insurance to healthcare to video recommendation systems. Especially in the housing, health, hiring, and credit contexts, consumers are rarely aware of when a company is using an automated decision-making system, let alone capable of avoiding that system.[145] As the White House Office of Science and Technology Policy wrote in the introduction to its *Blueprint for an AI Bill of Rights*:

> "In America and around the world, systems supposed to help with patient care have proven unsafe, ineffective, or biased. Algorithms used in hiring and credit decisions have been found to reflect and reproduce existing unwanted inequities or embed new harmful bias and discrimination. Unchecked social media data collection has been used to threaten people's opportunities, undermine their privacy, or pervasively track their activity—often without their knowledge or consent. These outcomes are deeply harmful—but they are not inevitable."

When consumer data is used to train these automated decision-making systems, any flaws, biases, or inaccuracies in the data can perpetuate or exacerbate the consumer privacy harms that automated systems produce.[146] For example, students can be subjected to several forms of unavoidable automated decision-making at school, including surveillance, exam monitoring, and

[144] *See* EPIC Commercial Surveillance FTC Comments at 86, 94; *cf.* Sherman, *supra* note 75.
[145] EPIC Commercial Surveillance FTC Comments at 75; *see also* Ari Ezra Waldman, *Power, Process and Automated Decision-Making*, 88 Fordham L. Rev. 613, 615–16 (2019) ("Using algorithms to make commercial and social decisions is really a story about power, the people who have it, and how it affects the rest of us.").
[146] These harms mirror the variety of privacy harms discussed by Danielle K. Citron and Daniel J. Solove. *See* Citron & Solove, *supra* note 115.

communications screening on school-mandated laptops,[147] which can force them to restrict or regulate their behavior, and which may incorrectly place students' academic standing in jeopardy.[148] Consumers can lose out on valuable job opportunities because of determinations made by untested and unproven automated hiring algorithms like those used by HireVue.[149] Historical racism and bias can be reflected in consumer data, leading to the creation of automated decision-making systems that perpetuate racial biases across industries and applications.[150] And in the financial industry, loan servicers and refinancers like Upstart can use automated decision-making systems to inject "alternative data" from commercial databases into the loan decision process—data outside the scope of information normally considered in loan decisions, and data ultimately used to make discriminatory lending decisions.[151] These systems impact every consumer they interact, effectively extending the risk of privacy harms and the harms of inaccurate data even to consumers whose data was not collected or used to train the systems.

[147] EPIC Consumer Surveillance FTC Comments at 70; Charlie Warzel, *Welcome to the K-12 Surveillance State*, N.Y. Times (July 2, 2019), https://www.nytimes.com/2019/07/02/opinion/surveillance-state-schools.html.
[148] *Id.*; *see also* Kashmir Hill, *Accused of Cheating by an Algorithm, and a Professor She Had Never Met*, N.Y. Times (May 27, 2022), https://www.nytimes.com/2022/05/27/technology/college-students-cheating-software-honorlock.html.
[149] EPIC Consumer Surveillance FTC Comments at 71; Complaint and Request for Investigation, Injunction, and Other Relief, *In re HireVue* (Nov. 6, 2019), https://epic.org/wp-content/uploads/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.
[150] EPIC Consumer Surveillance FTC Comments at 73; *see also* Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, arXiv (Apr. 3, 2019), https://arxiv.org/abs/1904.02095; U.S. Gov't Accountability Off., GAO-21-519SP, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities (2021), https://www.gao.gov/products/gao-21-519sp; Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage Health of Populations*, 366 Sci. 447 (2019).
[151] EPIC Consumer Surveillance FTC Comments at 72; Press Release, NAACP Legal Def. & Educ. Fund, NAACP Legal Defense and Educational Fund and Student Borrower Protection Center Announce Fair Lending Testing Agreement with Upstart Network (Dec. 1, 2020), https://www.naacpldf.org/press-release/naacp-legal-defense-and-educational-fund-and-student-borrower-protection-center-announce-fair-lending-testing-agreement-with-upstart-network/.

IV. Existing Regulations and Mechanisms

a. The failure of current law and enforcement to protect consumers from data brokers

The following is responsive to Questions 13, 17, and 21.

Existing regulations and mechanisms are inadequate to protect consumers from data broker-facilitated harms. Current protections are limited in scope; they put the burden on consumers and result in predictably inequitable outcomes, concentrate market power, fail to create transparency, and fail to address downstream misuse.

In the United States in 2023, certain types of consumer information are still practically unprotected. As an initial matter, because the United States is without a comprehensive privacy law, certain types of information are simply "out-of-scope" of key consumer protection frameworks. At a recent House Energy and Commerce hearing on the opacity of data broker practices, for example, witnesses testified that the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[152] does not typically protect data about purchasing laxatives or yeast infection medication,[153] and that brokers circumvent the Children's Online Privacy Protection Act (COPPA)[154] by getting information about teenagers aged 13 to 17[155] or about households in which there are parents of children who are

[152] Pub. L. No. 104-191, 100 Stat. 2548 (1996) (implemented by U.S. Department of Health and Human Services at 45 C.F.R. pts. 160, 164) (implemented via the FTC's Health Breach Notification Rule at 16 C.F.R. pt. 318).
[153] *See, e.g.*, *Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy: Hearing Before the Subcomm. of Oversight and Investigations of the H. Comm. on Energy & Com.*, 118th Cong. 55.20 (2023), https://docs.house.gov/meetings/IF/IF02/20230419/115788/HMTG-118-IF02-Bio-MoyL-20230419.pdf (testimony of Laura Moy, Associate Professor of Law, Georgetown University Law Center) [hereinafter "Moy Testimony"].
[154] 15 U.S.C. §§ 6501–06; *See Complying with COPPA: Frequently Asked Questions*, FTC, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited July 11, 2023) ("The Rule was designed to protect children under age 13").
[155] *See Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy: Hearing Before the Subcomm. of Oversight and Investigations of the H. Comm. on Energy & Com.*, 118th Cong. 44.30 (2023), https://www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Bio-ShermanJ-20230419.pdf (testimony of Justin Sherman, Senior Fellow and Research Lead, Data Brokerage Project) [hereinafter "Sherman Testimony"].

under age 13.[156] Use of sensitive health-related data is both long known and still shocking, including the sale of mental health data,[157] the dissemination of location data surrounding visits to Planned Parenthood,[158] the disclosure of health information to a non-HIPAA-covered third party such as a gym or a website like WebMD,[159] the drawing of inferences about health and/or location derived from other types of data,[160] and the linking of information to an individual's device[161] through methods such as browser fingerprinting (which can include something as innocuous as what fonts a consumer has installed).[162] Last year, the Markup uncovered that 33 of the 100 top hospitals shared data (including patient's IP address, doctor's name, and reason for the appointment) with Meta, the parent company of Facebook, through online tracking tools called pixels.[163] Notably, even when attempting to create stronger protections from data brokers for judges, Congress exempted entities

[156] *See id.* at 44.12.
[157] *See, e.g.*, Kim, *supra* note 10, at 20–21.
[158] *See* Cox, *supra* note 13.
[159] *See* Pam Dixon & Robert Gellman, World Priv. F., The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future 15 (Apr. 2, 2014), https://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf [hereinafter "WPF Report"] (noting that after a consumer reveals his or her health information to a non-HIPAA third party, that information is considered out of HIPAA's bounds); *id.* at 62 (e.g., gym); *id.* at 68 (WebMD score); *id.* at 15, 62, 68 (website), *id.* at 65–66 (non-clinical frailty score).
[160] *See, e.g.*, Sherman Testimony at 38.30 (discussing inferences that can be made about health and location without technically collecting those types of data).
[161] *See, e.g.*, *id.* at 1.07.20 (noting that broker may not be collecting name but data collected may link to device).
[162] *See, e.g.*, *Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy: Hearing Before the Subcomm. of Oversight and Investigations of the H. Comm. on Energy & Com.*, 118th Cong. 1.12.10 (2023), https://www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Wstate-ErwinM-20230419.pdf (testimony of Marshall Erwin, Chief Security Officer at Mozilla) [hereinafter "Erwin Testimony"].
[163] *See, e.g.*, Todd Feathers et al., *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites. A recent Senate report exposed similar pixel-enabled abuses on tax websites. *See* Makena Kelly, *Democrats call on DOJ to investigate tax sites for sharing financial information with Meta*, The Verge (July 12, 2023), https://www.theverge.com/2023/7/12/23791496/meta-google-tax-filing-warren-sanders-pixel.

subject to FCRA from having to comply with these heightened safeguards.[164] FCRA deficiencies (and correspondingly opportunities to use FCRA to better protect consumers) are discussed in greater detail below. As these examples illustrate, there are significant gaps and shortcomings in the existing privacy framework(s), especially as relates to data brokers.

Historically, opt-in and opt-out privacy regimes have been premised on the legal fiction that consumers read, understand, and accept a company's (or website's) terms and conditions and/or privacy policy—this model of protecting privacy was dubbed 'notice and consent' or 'notice and choice.'[165] There is significant evidence to suggest that this regime does not effectively serve as notice nor effectively provide consumers with a choice.[166] However, because consumers do not have a direct relationship with data brokers, consumers often don't even benefit from an outdated and burdensome notice-and-choice approach to privacy when it comes to data brokers using data about them.[167] Indeed, this opacity is sometimes maintained deliberately and contractually.[168]

[164] *See EPIC Statement Expressing Concerns on the Inclusion of the Judicial Security and Privacy Act in the NDAA*, EPIC (Dec. 13, 2022), https://epic.org/epic-statement-expressing-concerns-on-the-inclusion-of-the-judicial-privacy-and-security-act-in-the-ndaa/.
[165] *See, e.g.*, CR EPIC Data Minimization Whitepaper at 15 (citing Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018); Neil Richards, Why Privacy Matters (2021)).
[166] *See, e.g., id.*; *see also* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & Pol'y for Info. Soc'y 543 (2008); WPF Report at 15 ("A buried statement in an unread privacy policy that "we may share your information for marketing purposes with third parties" is not informed consent to allow unfettered use information for predictive scoring").
[167] *See, e.g.*, Rebecca Kelly Slaughter, Comm'r, FTC, The FTC's Approach to Consumer Privacy 1 (Apr. 10, 2019), https://www.ftc.gov/system/files/documents/public_statements/1513009/slaughter_remarks_at_ftc_approach_to_consumer_privacy_hearing_4-10-19.pdf; FTC, *Protecting Consumer Privacy in an Era of Rapid Change* iii (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf; Press Release, EPIC, EPIC to House Committee: Notice and Choice Does Not Protect Privacy (Feb. 27, 2023), https://epic.org/epic-to-house-committee-notice-and-choice-does-not-protect-privacy/.
[168] *See, e.g.*, Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* 173 (2016) (noting data brokers are immune from market incentives to promote privacy) (citing Senate Data Broker Report at iii) ("Data brokers typically amass data without direct interaction with consumers, and a number of the queried brokers perpetuate this secrecy by contractually limiting consumers from disclosing their data services").

Even in the limited circumstances in which sectoral privacy laws actually do apply, they often put a disproportionate burden on consumers.[169] They sometimes allow for pay-for-privacy regimes,[170] which clearly create inequitable outcomes, especially for vulnerable populations for whom the privacy expense is more costly.[171] Simply put: not every consumer has the time and energy necessary to identify, understand, and take persistent action to correct or delete personal data held by a data broker, and no consumer should have to opt out more than once. (Arguably the consumer should have to opt in rather than opt out, and ideally principles of data minimization[172] would automatically apply, limiting what information was even possible to collect.) The cottage industry that has popped up to offer privacy from data brokers is subscription-based in no small part because of this reality; brokers can acquire and use your data again even after you've told them to

[169] *See* Daniel J. Solove, *The Limitations of Privacy Rights*, 98 Notre Dame L. Rev. 975, 975 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4024790 ("[privacy] rights put too much onus on individuals when many privacy problems are systematic").

[170] *See, e.g.*, Aaron Rieke et al., Upturn, Open Soc'y Founds., Data Brokers in an Open Society 37 (2016), https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf [hereinafter "OSF Data Brokers Report"] ("Vehicles from low-income communities are overrepresented in these databases compared to those from rich, gated communities. This makes it far easier for law enforcement to track the whereabouts of low-income individuals, simply because of how data brokers buy and assemble data"). It also stands to reason that that those with disposable income will be over-represented among consumers who use subscription-based opt-out vendors.

[171] *See, e.g.*, CFPB Advisory Opinion on Fair Credit Reporting; Facially False Data, 87 Fed. Reg. 64689, 64692 (Oct. 26, 2022), https://www.federalregister.gov/documents/2022/10/26/2022-23264/fair-credit-reporting-facially-false-data [hereinafter "CFPB Facially False Data Opinion"] ("This risk may be even more acute for minors in the United States foster care system, who often lack a permanent address and frequently have their personal information shared among numerous adults and agency databases, making them particularly susceptible to identity theft and inaccurate credit history information") (citing Press Release, CFPB, CFPB Releases Tools to Protect Foster Care Children from Credit Reporting Problems (May 1, 2014), https://www.consumerfinance.gov/about-us/newsroom/cfpb-releases-tools-to-protect-foster-care-children-from-credit-reporting-errors/; Amanda Manes, *What Steps Can Survivors Take to Repair Credit Damaged by Abusers?*, VAWnet News Blog (Dec. 29, 2015), https://vawnet.org/news/what-steps-can-survivors-take-repair-credit-damaged-abusers.

[172] *See, e.g.*, CR EPIC Data Minimization Whitepaper; Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers*, EPIC Blog (May 4, 2023), https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/.

delete it.[173] This is particularly problematic when coupled with the chronic inaccuracies pervasive in the industry, such as reporting outdated derogatory information,[174] lack of accountability for ensuring accuracy,[175] reported accuracy rates well below 60%,[176] and inaccuracies resulting from missing data (especially in criminal records).[177] In other contexts, forcing consumers to navigate this kind of whack-a-mole obstacle course to control their personal data would be characterized as outright fraud.[178]

[173] *See* Zachary McAuliffe, *Data Brokers and Personal Deletion Services: What You Should Know*, CNET (Feb. 22, 2023), https://www.cnet.com/tech/services-and-software/data-brokers-and-personal-data-deletion-services-what-you-should-know/ ("There is also no way to check if data brokers comply with these requests to delete your information. Personal data deletion services, to their credit, say as much on their websites…. The reason these services are subscription based rather than one-time uses is because data brokers and people finder sites can still get your information after it's been deleted.").

[174] *See, e.g.*, CFPB Facially False Data Opinion at 5 (noting CFPB has brought enforcement actions in response to inherent logical inconsistencies); *id.* at 7 (noting as an inconsistency derogatory information in a report when that information predates an earlier report that did not include the information).

[175] *See, e.g.*, FTC Data Brokers Report at i ("The contracts between data brokers and their clients include few provisions regarding the accuracy of their products. Some of the data brokers represent to their clients that their information is only as accurate as their sources and accept no responsibility to validate the accuracy of their data.").

[176] *See, e.g.*, John Lucker et al., *supra* note 18, at 21 (noting more than two-thirds of survey respondents stated that the third-party data about them was only 0 to 50 percent correct as a whole, one-third of respondents perceived the information to be 0 to 25 percent correct); Henrik Twetman & Gundars Bergmanis-Koratz, NATO Strategic Commc'ns Ctr. Excellence, Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data 14 (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf ("Our research indicates that quantity overshadows quality in the data broker industry, and that on average only 50–60% of data can be considered precise.").

[177] *See, e.g.*, OSF Data Brokers Report at 170 ("Missing data can also paint an inaccurate picture: a record that indicates a pending felony charge has different consequences than one with a felony charge followed by a "not guilty" disposition; criminal records may list the same offense multiple times, or fail to remove expunged or outdated convictions, irrelevant arrests, or include cases in which charges were ultimately dropped"); Rebecca Oyama, *Do Not (Re)Enter: The Rise of Criminal Background Tenant Screening as a Violation of the Fair Housing Act*, 15 Mich. J. Race & L. 181, 188 (2009).

[178] *See, e.g.*, Cyrus Farivar, *All of Mugshots.com's Alleged Co-owners Arrested on Extortion Charges*, Ars Technica (May 17, 2018), https://arstechnica.com/tech-policy/2018/05/all-of-mugshots-coms-alleged-co-owners-arrested-on-extortion-charges/; Brooke Rink, *If a Picture Is Worth a Thousand Words, Your Mugshot Will Cost You Much More: An Argument for Federal Regulation of Mugshots*, 73 Fed. Commc'ns L. J. 317 (2021).

The data broker industry is characteristically without transparency. It is a model that is explicitly ***not*** built on direct relationships with the consumers whose data it sells,[179] and an industry which both regulators and legislators struggle to penetrate the inner workings of. For example, it is difficult to distinguish between data points like "biker" or "diabetes interest" or "smoker in household" being used for targeted ads rather than increased insurance rates.[180] Data brokers buy and sell data from one another so frequently (including inferred or predicted data) that it would be unfeasible to fully account for how some brokers obtain their data.[181] This makes it difficult to detect violations and enforce against them, as well as to equip consumers to protect themselves from this conduct.[182] Indeed, consumers' attempts to protect themselves may be actively circumvented.[183]

This lack of transparency not only complicates enforcement and consumer education but also allows for cascading harms through downstream misuse of consumer data. Misuse can include

[179] *See, e.g.*, FTC Data Brokers Report at v ("Consumers may not be aware that data brokers are providing companies with products to allow them to advertise to consumers online based on their offline activities"); Coalition Letter to CFPB Requesting Broad Consumer Financial Market Correction, Beginning with an Advisory Opinion Regarding Credit Header Data 3 (Feb. 8, 2023), https://www.nclc.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf [hereinafter "Coalition Letter to CFPB"] ("Data brokers buy and sell hundreds of millions of names and addresses gathered by essential utilities companies without consumers' knowledge or consent").

[180] *See* FTC Data Brokers Report at v–vi, 24–25, 55–56 (noting challenges with ensuring risks are mitigated and marketing information is not used for other purposes (e.g., "biker," "diabetes interest," or "smoker in household" categories used for increased insurance premiums or credit risks rather than targeted ads)).

[181] *See, e.g.*, OSF Data Brokers Report at 170 (popular websites will frequently result in the exchange of data with tens, or even hundreds, of behind-the-scenes trackers that record the websites a particular internet user has visited).

[182] *See, e.g.*, Hoofnagle, *supra* note 168, at 174 ("The lack of rights and secrecy involved also means that data brokers can sell data to scam artists or other unseemly businesses."). EPIC notes that piecemeal enforcement efforts after the fact are not equal to the challenge of such a systemic problem.

[183] *See, e.g.*, Joel Reardon et al., *50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions' System*, 28th USENIX Sec. Symp. (2019), https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf; Liam Tung, *Think You've Switched Off Android Tracking? Apps are Logging Your Movements Anyway*, ZDNet (July 9, 2019), https://www.zdnet.com/article/think-youve-switched-off-android-tracking-apps-are-logging-your-movements-anyway/.

purchase by law enforcement (especially for purposes of detention or deportation),[184] marketing predatory products to low-income communities of color,[185] and threats to physical safety.[186] These misuses can result in privacy harms, as well as reputational, emotional, physical, and economic harms.[187] In the absence of adequate regulation, these misuses should be expected, as a result of selling criminal records[188] and other information without taking reasonable steps to prevent them from being used for impermissible purposes (including failing to require downstream users to identify themselves and their purpose for seeking the information).[189] Even where federal regulators

[184] *See, e.g.*, *Fighting Back Data Brokers*, Just Futures Law, https://www.justfutureslaw.org/fighting-data-brokers (last visited July 11, 2023); Just Futures Law, Reply Comments in the Matter of Data Breach Reporting Requirements, WC Docket No. 22-21 10 (Mar. 24, 2023), https://www.fcc.gov/ecfs/document/10325231325541/1; M. Jos. Capkovic, *Our Walls in the Information Age*, 5 Critical Stud. J. 1, 12–13 (2012) (noting FBI offered reasoning for why commercial data brokers are not subject to FCRA); OSF Data Brokers Report at 170 (addressing marketing data put to non-marketing uses, for example, government surveillance efforts piggybacking on commercial data collection activities by data brokers).

[185] *See, e.g.*, Coalition Letter to CFPB at 4 ("data brokers may sell information about low-income communities of color to entities that will use that information to market predatory products, such as high-interest payday loans").

[186] *See, e.g.*, Joseph Cox, *T-Mobile 'Put My Life in Danger' Says Woman Stalked with Black Market Location Data*, 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; *Data Brokers: What They Are and What You Can Do About Them*, Nat'l Network to End Domestic Violence, https://www.techsafety.org/data-brokers (last visited July 11, 2023); Robertson, *supra* note 130.

[187] *See, e.g.*, Permissible Purposes for Furnishing, Using, and Obtaining Consumer Reports, 87 Fed. Reg. 41243, 41244 (July 12, 2022), https://www.consumerfinance.gov/rules-policy/final-rules/fair-credit-reporting-permissible-purposes-for-furnishing-using-and-obtaining-consumer-reports/ ("The FCRA's permissible purpose provisions are thus central to the statute's protection of consumer privacy. Consumers suffer harm when consumer reporting agencies provide consumer reports to persons who are not authorized to receive the information or when recipients of consumer reports obtain or use such reports for purposes other than permissible purposes. These harms include the invasion of consumers' privacy, as well as reputational, emotional, physical, and economic harms"). We offer additional examples in discussing data security below.

[188] *See, e.g.*, Press Release, FTC, FTC Approves Final Order Settling Charges Against Marketers of Criminal Background Screening Reports (May 1, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/05/ftc-approves-final-order-settling-charges-against-marketers-criminal-background-screening-reports (finalizing order against company that failed to inform customers about obligations for use of criminal record reports).

[189] *See, e.g.*, Press Release, FTC, Two Data Brokers Settle FTC Charges That They Sold Consumer Data Without Complying With Protections Required Under the Fair Credit Reporting Act (Apr. 9, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/04/two-data-brokers-settle-ftc-charges-they-sold-consumer-data-without-complying-protections-required (taking action under FCRA against companies that provided consumer reports without taking reasonable steps to make sure users had a permissible reason to

have had explicit rules governing the proper safeguards for consumer data, they have failed to prevent downstream misuse.[190] Again, this seems to be a function of lack of transparency, which leads to challenges in detecting violations.[191]

The data broker industry implicates competition concerns as well. Law Professor Sarah Lamdan references companies like RELX and Thomson Reuters as occupying "the top of the personal data food chain", possessing dossiers on more than two-thirds of U.S. residents.[192]

b. Specific existing mechanisms

The following is responsive to Questions 17 and 21.

i. Public sector mechanisms apart from the Bureau's own authorities

We address recommendations to the Bureau below. In this section, we briefly touch upon other federal and state laws and regulations that may pertain to the data broker industry. It is important to note at the outset that in many instances, data brokers have data-sharing pipelines and agreements that extend beyond the strict activity of a "sale," and so the Bureau should consider a more expansive definition of the misconduct it is attempting to prevent as it considers how to best protect consumers from data brokers.[193]

---

have them, for example not requiring users to identify themselves nor their purpose for obtaining the reports); Sherman Testimony at 52.50 (noting that brokers don't vet who they sell to).

[190] CPNI rules failed to prevent telephone carriers from facilitating the egregious sale of location data of millions of Americans by entities like Securus. *See, e.g.*, *In re AT&T Inc.*, File No.: EB-TCD-18-00027704 (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf; WPF Report at 22 n.27 ("The FTC has brought cases around "mission creep" in the use of credit score outside of its regulated uses").

[191] *See* FTC Data Brokers Report at 55–56 ("[T]he Commission recommends that data brokers take reasonable precautions to ensure that downstream users of their data do not use it for eligibility determinations or for unlawful discriminatory purposes. For example, while the data segment of "Smoker in Household" could be used to market a new air filter, a downstream entity also could use the segment to suggest that a person is a poor credit or insurance risk…").

[192] Coalition Letter to CFPB at 2 (citing Sarah Lamdan, Data Cartels: The Companies That Control and Monopolize Our Information (2022)) ("Companies like RELX and Thomson Reuters, which one scholar describes as occupying "the top of the personal data food chain," possess dossiers on millions of people, including more than two-thirds of U.S. residents").

[193] *See* Justin Sherman, *Federal Privacy Rules Must Get "Data Broker" Definitions Right*, Lawfare (Apr. 8, 2021), https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right.

There is currently no comprehensive privacy law at the federal level, however the framework presented in the proposed American Data Privacy and Protection Act (ADPPA) is encouraging.[194] ADPPA would include strict data minimization obligations that would dramatically curtail current data broker business models; global and individual opt-out provisions from data collection; and a Do Not Collect registry that would both require deletion of already-collected data and prohibit new data from being collected unless affirmative express consent is obtained from the consumer.[195]

One admitted shortcoming of the data broker laws in California and Vermont is that the penalties for violations are minimal. For example, in Vermont, the fine for failing to register is $50 per day, to a maximum of $10,000 per year.[196] In California, the fine is $100 per day with no such maximum (but still well below $40,000 per year).[197] Additional costs can be assessed (such as the cost of investigation and prosecution of violations), and Vermont has already brought enforcement actions against companies violating its data broker registry law.[198] However the law has been described as a "basic transparency measure"[199] rather than a true remedy to the data broker problem. Indeed, these laws seem both to fall short as a deterrent and often put the onus on the consumer. As we discuss below, we encourage the CFPB to consider how it can use its authority under FCRA to reverse that burden and put the onus on the parties profiting from this use of consumer data. This is

[194] H.R. 8152, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text [hereinafter "ADPPA"]; *see also* Press Release, EPIC, EPIC Joins 48 Public Interest Groups Urging House to Vote on American Data Privacy and Protection Act (Aug. 25, 2022), https://epic.org/epic-joins-48-public-interest-groups-urging-house-to-vote-on-american-data-privacy-and-protection-act/.
[195] ADPPA § 101 (data minimization); ADDPA § 204 (opting out, including opting out of targeted advertising); ADDPA § 206 (Do Not Collect).
[196] Vt. Stat. Ann. Tit. 9, § 2246 (2019).
[197] Cal. Civ. Code § 1798.99.82(c)(1)(A).
[198] *See, e.g.*, Christian Hetrick, *N.J. Data Broker Tried to Sell Personal Info on a Million Kids but Didn't Tell State Officials* (Mar. 19, 2019), https://www.inquirer.com/business/technology/alc-princeton-data-broker-personal-info-million-kids-vermont-law-20190319.html; Press Release, Off. Vt. Att'y Gen., Attorney General Wins Significant Victory in Clearview AI Lawsuit (Sept. 11, 2020), https://ago.vermont.gov/blog/2020/09/11/attorney-general-wins-significant-victory-clearview-ai-lawsuit.
[199] IAPP, *Vt. Data broker law producing subtle results* (Jan. 10, 2020), https://iapp.org/news/a/vt-data-broker-law-producing-subtle-results/.

especially important as many state comprehensive privacy laws do not apply when FCRA applies.[200] While some states[201] (and even municipalities)[202] have their own "mini-FCRAs," not all states do, and they are not identical to FCRA, which the CFPB has expressly allowed for.[203]

ii. Industry, nonprofit, and private sector mechanisms

Other mechanisms have been deployed to rein in the data broker industry, such as industry self-regulation, companies offering data deletion services either as an added perk for their customers or as a standalone subscription-based offering, and nonprofits offering technical support to consumers in exercising their rights. However, each of these also fall short of what is required to adequately protect consumers.

The Network Advertising Initiative (NAI) has set up an opt-out page that is entirely voluntary and offers no guarantee of being functional.[204] Per the Bureau's rules, if this is the only online method to opt-out from a given broker's use of consumer data and the broker does not provide a link to the NAI webpage to do so, that opt-out mechanism would not be considered "reasonable and simple."[205] We further note that there are numerous instances of credit reporting

[200] *See, e.g.*, Cal. Civ. Code § 1798.145(d)(2); Colo. Rev. Stat. § 1-6-1-1304(2)(i); Conn. Gen. Stat. § 42-517(b)(11); Ind. Code § 24-15-1-1(2); Va. Code. Ann. § 53-59.1-576(C)(10); Tex. Ins. Code tit. 5, § 541.003(11).
[201] *See, e.g.*, N.Y. Gen. Bus. Law § 380 (2022); Ga. Code § 10-1-390 *et seq.* (2022); Okla. Stat. tit. 24, § 147 (2022); Wash. Rev. Code § 19.182.005 *et seq.* (2022); Me. Stat. tit. 10, Stat § 1306 (2022); Minn. Stat. § 13C.02 (2022).
[202] *See, e.g.*, Press Release, City of New York, Mayor de Blasio and Human Rights Commissioner Malalis Announce New Law Taking Effect Today to Protect New Yorkers Against Employment Discrimination Based on Credit History (Sept. 3, 2015), https://www.nyc.gov/office-of-the-mayor/news/591-15/mayor-de-blasio-human-rights-commissioner-malalis-new-law-taking-effect-today-to.
[203] *See* The Fair Credit Reporting Act's Limited Preemption of State Laws, 87 Fed. Reg. 41042 (July 11, 2022), https://www.consumerfinance.gov/rules-policy/final-rules/the-fair-credit-reporting-acts-limited-preemption-of-state-laws/.
[204] *See Opt Out of Interest-Based Advertising*, Network Advertising Initiative, https://optout.networkadvertising.org/?c=1 (last visited July 12, 2023) ("The NAI opt-out page is provided as a convenience to the public, but the opt-out cookie is set by participating NAI members, who are solely responsible for setting opt-out cookies and honoring your requests. Because no technology is perfect, neither NAI nor its members warrant that the opt-out tool will be error-free or always work as intended.").
[205] 12 C.F.R § 1022.25(b)(2)(iii).

companies exhibiting egregious deficiencies in their obligations to consumers, which seems to counsel against relying on a model of industry self-regulation.[206]

Subscription-based opt-out services[207] or companies that offer data deletion as a perk to existing customers[208] may help[209] those with sufficient disposable income to afford them, but even setting aside equity issues, it is backwards to allow companies to profit from consumer data until such time and for as long as the consumer spends their own money to stop it.

Consumer Reports has built a tool called Permission Slip premised on the ability to act as an 'authorized agent' for consumers under the California Consumer Privacy Act (CCPA).[210] However, as of March 2022, companies honored fewer than 25% of Permission Slip's requests for access to a consumer's data.[211] In April 2023, Consumer Reports offered recommendations on how companies can make it easier for authorized agents to act on behalf of the consumers they are trying to assist, including extending the timeout on request forms from 3 minutes to 10 minutes.[212] But even well-

[206] *See, e.g.*, Hoofnagle, *supra* note 168, at 274 (FTC sued CRAs because they didn't answer their phones); *id.* at 274–75 (additional misconduct); *id.* at 277–78 (misuse of credit header data); Darian Dorsey, Hold Credit Reporting Companies Accountable for Incorrect Reports and Shoddy Service, CFPB Blog (Apr. 19, 2022), https://www.consumerfinance.gov/about-us/blog/hold-credit-reporting-companies-accountable-incorrect-reports-shoddy-service/; Ryan Sandler, CFPB, Disputes on Consumer Credit Reports (2021), https://www.consumerfinance.gov/data-research/research-reports/disputes-on-consumer-credit-reports/.
[207] *See* McAuliffe, supra note 173.
[208] *See, e.g.*, Press Release, Discover, Discover Launches Free Benefit to Help Customers Remove Personal Information From 10 Popular Data-Collecting Websites (Apr. 20, 2022), https://investorrelations.discover.com/newsroom/press-releases/press-release-details/2022/Discover-Launches-Free-Benefit-to-Help-Customers-Remove-Personal-Information-From-10-Popular-Data-Collecting-Websites/default.aspx.
[209] Even then, they may only be useful for certain public facing sites—and may not go into enough detail for data broker datasets.
[210] *See Permission Slip*, Consumer Reps., https://innovation.consumerreports.org/initiatives/permission-slip/ (last visited July 14, 2023).
[211] *See* Kaveh Waddell, *How 'Authorized Agents' Plan to Make It Easier to Delete Your Online Data*, Consumer Reps. (Mar. 21, 2022), https://www.consumerreports.org/privacy/authorized-agents-plan-to-make-it-easier-to-delete-your-data-a8655835448/.
[212] *See* Ann Marie Carrothers, *Recommendations to Companies for their Authorized Agent Forms*, Consumer Reps. (Apr. 27, 2023), https://innovation.consumerreports.org/recommendations-to-companies-for-their-authorized-agent-forms/.

designed tools and systems for consumers to exercise access, correction, and deletion rights cannot account for the lack of those rights under the laws of most states.

Unfortunately, current public sector remedies often amount to little more than extracting a toll from data brokers, and private sector remedies are inadequate to the scale of the problem. This stands in marked contrast to contexts in which data controllers are subject to express and effective privacy regulations backed by meaningful enforcement.[213] Earlier this year, enforcement actions regarding pixel tracking in telehealth[214] and on health websites, including an explicit clarification about breach reporting requirements from the FTC, spurred prompt action from the health industry.[215] (A few providers had taken action last year in response to investigative reporting.[216])

V. EPIC's Recommendations to the CFPB

The following is responsive to Question 22.

a. Overarching principles for the Bureau's regulation of data brokers

In addition to the specific recommendations we outline below, we urge the Bureau to prioritize three overarching principles: prioritizing the individual rights of consumers over protecting the business practices of data brokers; data minimization; and data security.

We applaud the Bureau's attention to the systemic problems created by data brokers. While we support a private right of action to empower consumers to enforce their rights, we agree with

[213] *See, e.g.*, *Summary of the HIPAA Privacy Rule*, U.S. Dep't Health & Hum. Servs. (Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (noting annual cap of $25k-$1.9MM, criminal penalties). HIPAA's scope is narrower than many consumers might expect. For example, health-related apps, laxative medications, and yeast infection medications are often not covered by HIPAA. *See, e.g.*, Moy Testimony at 55.20.

[214] *See* Carly Page, *The Crackdown on Pixel Tracking in Telehealth is a Warning for Every Startup*, TechCrunch (Apr. 17, 2023), https://techcrunch.com/2023/04/17/pixel-tracking-hipaa-startups/.

[215] *See* Ruth Reader, *'Shut It Off Immediately': The Health Industry Responds to Data Privacy Crackdown*, Politico (Apr. 17, 2023), https://www.politico.com/news/2023/04/17/health-industry-data-privacy-00092447 (protected data can include email addresses, IP addresses, or geographic location information that can be tied to an individual…FTC said entities not covered by HIPAA that collect personally identifiable health information must tell consumers when there's been a breach of their data).

[216] *See* Nicole Wetsman, *Hospital Websites are Sending Medical Information to Facebook*, Verge (June 16, 2022), https://www.theverge.com/2022/6/16/23170886/hospital-websites-meta-pixel-tracker-facebook-hipaa.

Professor Daniel Solove that the solution cannot rest ***solely*** in rights that each individual consumer will have the burden of invoking.[217] Consumers shouldn't be stuck playing a game of "red light green light"[218] every time they turn their attention away from an entity with access to their data. Especially as each household may have to identify and engage with thousands of different data broker companies, making individual requests for each member of their family, each time, in order to exercise their rights.[219] In some instances, the consumer never intended for their data to be shared in this way,[220] may have taken affirmative steps to prevent their data from being shared which have been disregarded,[221] and in other instances, the consumer may not even know that their information is exposed in someone else's record.[222] This problematic lack of autonomy over their own data is

[217] *See* Solove, *supra* note 169, at 975 ("[Privacy] rights put too much onus on individuals when many privacy problems are systematic").
[218] *See Statues (game)*, Wikipedia, https://en.wikipedia.org/wiki/Statues_(game) (last visited July 12, 2023).
[219] *See, e.g.*, Sherman Testimony at 57.53.
[220] *See, e.g.*, *In re Urth Access, Inc.*, File No. EB-TCD-22-00034232, ¶ 15 (Dec. 8, 2022), https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls ("The websites included TCPA consent disclosures whereby the consumer agreed to receive robocalls from 'marketing partners.' These 'marketing partners' would only be visible to the consumer if the consumer clicked on a specific hyperlink to a second website that contained the names of each of 5,329 entities. We find that listing more than 5,000 'marketing partners' on a secondary website is not sufficient to demonstrate that the called parties consented to the calls from any one of these 'marketing partners.'" (internal citations omitted).; Complaint at 6, *In re Everalbum, Inc.*, FTC File No. 192-3172 (2021), https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf (describing practices of collecting user facial biometric information while representing to users that no such data collection was occurring); Complaint at 6, *United States v. Facebook*, 456 F. Supp. 3d 115 (D.D.C. 2019) (No. 19-cv-2184), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf (same).
[221] *See, e.g.*, Reardon et al., *supra* note 183.
[222] *See, e.g.*, Complaint, *Ramirez et al. v. LexisNexis Risk Solutions*, 2022-CH-07984, ¶ 24 (Il. Cir. Ct. Aug. 16, 2022), https://borderlessmag.org/wordpress/wp-content/uploads/2023/03/Castellanos-et-al.-v.-LexisNexis-Risk-Solutions-Complaint-For-Filing.pdf (showing ability to search for "relatives" and "associates"); *id.* at ¶ 37 (noting additional charge for data on "associates" or "relatives"); Permissible Purposes for Furnishing, Using, and Obtaining Consumer Reports, 87 Fed. Reg. 41243, 41244 (July 12, 2022), https://www.consumerfinance.gov/rules-policy/final-rules/fair-credit-reporting-permissible-purposes-for-furnishing-using-and-obtaining-consumer-reports/ (consumer reporting agencies violate the FCRA's permissible purpose provisions if they provide consumer reports on multiple consumers (e.g., when multiple consumers with the same last name appear in the same record due to name-only matching)); Chi Chi Wu et al., Nat'l Consumer L. Ctr., Fair Credit Reporting § 7.2.4.2 445 (10th ed. 2022) [hereinafter "NCLC FCR"] (employer may not obtain CR for individuals who are NOT the one they are making decision about, e.g. not relative of prospective employer).

often no fault of the consumer's, so it would be backwards to impose upon consumers the burden to solve it.

The Bureau should also prioritize principles of data minimization.[223] These principles include collecting only the data necessary to provide the service expected by the consumer, as well as limiting secondary uses of data to that which clearly serves the interests of consumers. In the case of data brokers, there is no guaranteed consumer expectation of benefit, only a hypothetical consumer interest in receiving more targeted advertising—and there are compelling reasons to believe that most consumers do not want this.[224] As such, we urge the Bureau to establish a presumption that when it comes to data brokers and consumer data, secondary uses are not in the consumer's interest. Data minimization also includes the timely disposal of information;[225] we urge the Bureau to consider how it might determine that proper disposal of data entails timely disposal,[226] working with the FTC as necessary.[227]

[223] *See* CR EPIC Data Minimization Whitepaper; Geoghegan, *supra* note 172.
[224] *See, e.g.*, Brooke Auxier et al., Americans Concerned, Feel Lack of Control Over Personal Data Collected by Both Companies and the Government, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/ ("At least eight-in-ten adults say they are at least a little concerned about how much personal information social media sites (85%), advertisers (84%), or companies they buy things from (80%) might know about them. The level of concern is felt most acutely when asked about social media sites or advertisers: About four-in-ten Americans say they have a lot of concern about how much personal information these respective groups have about them.") ("59% say they understand very little or nothing about what is being done with their data by companies").
[225] *See, e.g.*, Complaint, *In re Drizly, LLC*, FTC File No. 2023185, ¶ 13(f) (Oct. 24, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf (noting Drizly's failure to use reasonable information security practices included the failure to "[h]ave a policy, procedure, or practice for inventorying and deleting consumers' personal information stored on its network that was no longer necessary."); Complaint, *In re Chegg, Inc.*, FTC File No. 2023151, ¶ 9(f) (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf (similar allegation).
[226] *See* Moy Testimony at 45.33, 55.40.
[227] *See* Hoofnagle, *supra* note 168, at 285 ("The FTC retains authority over…§1681w, dealing with disposal of consumer report information").

Data security interests are served by data minimization practices as well;[228] data that is properly destroyed cannot be compromised. Given the numerous documented breaches of data brokers and of consumer reporting agencies, the Bureau's need to intervene is clear.[229] Breaches of consumer report data can be especially pernicious as the data is precompiled, pre-sorted, and ready for targeting by bad actors.[230] Beyond the immediate privacy and autonomy harms of a consumer having their data shared without their authorization (nor even with their knowledge, in many instances), there are downstream consequences as well. These could include using information to obtain access to other consumer accounts,[231] to commit fraud in the consumer's name,[232] or to physically harm, stalk, or harass the consumer.[233] On the other hand, improved data security can

[228] *See, e.g.*, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51277 (Aug. 22, 2022), https://www.federalregister.gov/d/2022-17752/p-88.
[229] *See, e.g.*, Brian Krebs, *Hacked Data Broker Accounts Fueled Phony COVID Loans, Unemployment Claims*, KrebsonSecurity (Aug. 6, 2020), https://krebsonsecurity.com/2020/08/hacked-data-broker-accounts-fueled-phony-covid-loans-unemployment-claims/ (2k files used to file for unemployment and SBA loans); Permissible Purposes for Furnishing, Using, and Obtaining Consumer Reports, 87 Fed. Reg. 41243, 41244 (July 12, 2022), https://www.consumerfinance.gov/rules-policy/final-rules/fair-credit-reporting-permissible-purposes-for-furnishing-using-and-obtaining-consumer-reports/ (describing 2006 FTC settlement with a consumer reporting agency, FTC alleged that agency violated the FCRA's permissible purpose provisions by providing consumer reports to persons without a permissible purpose, resulting in at least 800 cases of identity theft); Brian Krebs, *Data Broker Giant Hacked by ID Theft Service*, KrebsonSecurity (Sept. 25, 2013), https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/ (identity thieves masquerading as customers of ChoicePoint, obtained access to knowledge-based authentication (KBA) security questions).
[230] *See* Sherman Testimony at 53.20.
[231] *See, e.g.*, Brian Krebs, *Experian, You Have Some Explaining to Do*, KrebsonSecurity (July 11, 2022), https://krebsonsecurity.com/2022/07/experian-you-have-some-explaining-to-do/.
[232] *See, e.g.*, Letter from N.Y. Dep't Fin. Servs., Cybersec. Div., to Regulated Entitles regarding a Cyber Fraud (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.
[233] *See* Cox et al., *supra* note 186. *See also* Molly Martinez & Natalie Grim, *Proposed "Do Not Sell My Data" Bill Could Be Key for Domestic Violence Survivors*, Gray TV (Sept. 29, 2022), https://www.graydc.com/2022/09/29/proposed-do-not-sell-my-data-bill-could-be-key-domestic-violence-survivors/; Tom Kemp, *How SB 362 Can Protect Domestic Violence Victims' Online Information*, Tom's Blog (Apr. 24, 2023), https://www.tomkemp.ai/blog/2023/04/24/how-sb-362-can-protect-domestic-violence-victims-online-information ("As the California Judiciary Committee analysis of SB 362 states, it is "largely impractical for a consumer to navigate the systems of the hundreds of data brokers and to submit deletion requests individually to each." In light that there are hundreds of data brokers registered with California, a domestic violence victim would have to spend hundreds of hours to ensure that their address or location is deleted from data brokers' databases"); Sherman Testimony at 33.40 (ban sale of data in sensitive categories

mitigate not only the initial harms of a breach itself, but also downstream impacts such as subsequent identity theft and account compromise.

The suggestions we offer below are not meant to be exhaustive (we do not thoroughly address the Equal Credit Opportunity Act, for example), but are meant to give the Bureau inspiration for creative ways it might use its existing authorities to protect consumers from the well-documented harms caused and exacerbated by the data broker industry.

b. The Fair Credit Reporting Act

In 2011, the FTC expressed that the three chief goals of the FCRA were to (1) prevent the misuse of sensitive consumer information by limiting recipients to those who have a legitimate need for it; (2) improve the accuracy and integrity of consumer reports; and (3) promote the efficiency of the nation's banking and consumer credit systems.[234] We primarily address this first goal in our suggestions below; however, we note that accuracy issues can have severe repercussions for equity concerns.[235] Additionally, as a general matter, FCRA limits tort liability in exchange for fulfilling the safeguards and obligations of FCRA;[236] the Bureau should keep this relief tradeoff in mind as it considers how to interpret and enforce violations of FCRA.

(e.g., health, location) as presumptively harmful, due to stalking, doxing, etc.); *id.* at 58.07 (noting people search websites facilitate stalking (e.g., attacks on a judge's home), and are exempt from bills/privacy laws due to broad carveouts for publicly available info).

[234] FTC, 40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations 1 (2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf [hereinafter "2011 FTC Staff Summary"].

[235] *See, e.g.*, Hoofnagle, *supra* note 168, at 273 ("[O]nce this score falls below a certain range, the results are severe. The subprime market has much more costly credit, and sometimes these are plainly uneconomical deals. Subprime products are not only more costly, but their providers tend to prey on their customers with unexpected rules, fees, and limitations that consumers in the credit utopia never experience"); *but see also id.* at 273–74 (noting that credit reporting can reduce credit discrimination by shifting focus to more objective financial risk factors).

[236] *See* Hoofnagle, *supra* note 168, at 276 ("At the most basic level the FCRA creates a bargain for companies engaged in consumer reporting. If CRAs follow a wide range of safeguards, some specified, some not, to promote "maximum possible accuracy" and to limit disclosures, they enjoy limited immunity from state defamation, privacy, and negligence cases. However this bargain is beginning to fail.") (internal citations omitted).

For purposes of our comments, FCRA protects consumers by imposing requirements on consumer reporting agencies (CRAs) in the data collection, sharing, retention, and disposal they perform in the process of creating and disclosing consumer reports (CRs). FCRA defines a consumer report, with a few exceptions, as a communication of information by a CRA, bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for enumerated purposes such as credit, insurance underwriting, and employment.[237] The term "communication" and the seven consumer data categories are extremely broad; however, FCRA's definition of a consumer report is limited by the enumerated purposes. Generally, a CRA is a person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other consumer information, for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce to prepare or furnish consumer reports.[238] Again, engaging "in whole or in part in . . . assembling or evaluating…consumer information" is very broad, but the CRA definition too is limited by the purpose provision: furnishing consumer reports to third parties. In a digital world, the interstate commerce provision is not as limiting as it once was.

The definitions of CRA and consumer report make it clear that the scope of FCRA is very broad. Significantly, an entity does not need to use the information it collects for furnishing consumer reports 100% of the time to be considered a CRA—even 10% of the time could be sufficient.[239] And in at least one District Court, whether the entity actually ever shared the report was

[237] 15 U.S.C. § 1681a(d)(1).
[238] 15 U.S.C. § 1681a(f).
[239] *See* NCLC FCR § 2.3.5.3 45.

irrelevant to whether the data was considered a consumer report; the mere expectation of sharing the report was sufficient for the data to be treated as a consumer report.[240] While historically the FTC has viewed some data brokers as outside the scope of FCRA,[241] we urge the Bureau to recognize all data brokers as presumptively CRAs, unless they can demonstrate that they continuously undertake reasonable measures to prevent the data they collect and disclose from being used for any of FCRA's enumerated purposes. As we discussed above, downstream misuse of data, including the data that make up consumer reports, is a significant problem in the digital ecosystem, and the Bureau as uniquely positioned to address it.

Another reason data brokers should be presumptively subject to FCRA is because in many instances a broker's entire business model is built upon sharing third-party data. Even to the extent a broker shares first-party data, it is often combined with third-party data which should render the entire record subject to FCRA. We offer a quick example about first-party and third-party data to explain. Company A collects information about direct transactions between itself and a consumer (e.g., payments, product/service purchases, etc.), and shares that information with Company B (which is not a CRA)[242] for employment purposes. This is unlikely to be covered by FCRA, as the record is entirely a result of the company's direct transactions with its consumers; it is wholly first-party data. However, if Company B were to share that same information with Company C for

[240] *See* NCLC FCR § 2.3.1.2 33 n.35 (citing *Miller v. Trans Union*, 2013 WL 5442008 (M.D. Pa. Aug. 14, 2013) (actual transmission of report to third party is not necessary for it to be a consumer report, so long as it is expected to be used or collected for purposes of transmission), *adopted in part*, 2013 WL 5442059 (M.D. Pa. Sept. 27, 2013)). *Cf. Coulter v. Chase Bank*, 2020 WL 5820700, at *11 (E.D. Pa. Sept. 30, 2020) (summary judgment denied where defendant failed to provide authority for proposition that information appearing on consumer disclosure and alleged to ultimately impact consumer's report and score is not actionable under FCRA).

[241] *See, e.g.*, FTC Data Brokers Report at 1.

[242] This example gets more complicated if Company B is a CRA and the information is inaccurate in which case Company A could be liable under FCRA for furnishing inaccurate credit information to a CRA. *See e.g.*, Press Release, CFPB, CFPB Orders Hyundai to Pay $19 Million for Widespread Credit Reporting Failures (July 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-hyundai-to-pay-19-million-for-widespread-credit-reporting-failures/.

employment purposes (or for any of the enumerated purposes under FCRA), it should be covered by FCRA, as the data was not collected as a result of Company B's direct transaction history with the consumer (from Company B's perspective, it is third-party data).[243] Similarly, if Company A were to take that same transaction history and combine it with court records pertaining to that consumer (third-party data, from Company A's perspective) and share the combined record with Company B for employment purposes (or for any of the enumerated purposes under FCRA), that entire record would likely be covered by FCRA, as the record includes FCRA-covered data.

We organize our recommendations below into (i) what can be done more immediately through interpretive rules or enforcement, and (ii) what may (but not necessarily) require a more formal rulemaking process.

i. Interpretive rules and enforcement actions

The four recommendations below represent clarifications the Bureau can offer without needing to go through a formal rulemaking process regarding: (1) the broad scope of FCRA; (2) when a CRA becomes liable for misuse of a consumer report; (3) expectations for due diligence (or Know Your Customer (KYC) protocols); and (4) the holistic nature of consumer rights under FCRA, especially as relates to enjoying immunity to tort liability for FCRA-covered activities.

1. The broad scope of FCRA

The scope of what constitutes a consumer report under FCRA is much broader than how it has been historically construed. A dataset can constitute a consumer report for many reasons, including: the purpose for the collection or use of the data, the source of the data, and/or the inferences able to be drawn from the data. The Bureau should clarify explicitly that it takes a broad

[243] Note that Company A could share the same information with Company C without FCRA applying, just as easily as Company A could share it with Company B.

view of what constitutes a consumer report and offer multiple, varied, illustrative examples so that there is certainty in the marketplace about when FCRA applies and to whom.

For example, data that is expected to be used for a credit-related purpose or data that was initially collected for a credit-related purpose is subject to FCRA, even if that data is later applied to other purposes. FCRA applies even if the company is powering an algorithm using FCRA-covered data the company otherwise cannot directly access. This aligns with a federal district court determination that a national credit bureau's conduct was data collection covered by FCRA even where the credit bureau generated a score without "seeing" the underlying data that informed that score.[244] The court analogized to circuit court cases in which insurance companies investigating a claim using a pre-existing credit report from Equifax were subject to FCRA despite the fact that they were using the credit report for insurance claims and not credit- or underwriting-related purposes.[245]

The Bureau should take this approach—explicitly stating that data collected for a FCRA-related purpose or data expected to be used for a FCRA-related purpose is covered by FCRA even if repackaged in a non-FCRA-related report or ultimately used for non-FCRA-related purposes—in order to mitigate the issue of downstream misuse of data contained in credit reports, discussed above. It does not matter whether the FCRA-related purpose is the primary use or a secondary use—if one use constitutes a consumer report, then the data is considered a consumer report under FCRA.[246] A dataset containing information that was in a prior consumer report, even if the new dataset is not expected to be used for a FCRA-listed purpose can constitute a consumer report.[247] Any subsequent use of information that was originally collected in whole or in part for consumer

[244] *See Heagerty v. Equifax Info. Services LLC*, 447 F. Supp. 3d 1328, 1345 (N.D. Ga. 2020).
[245] *See id.* (citing *Yang v. Gov't Employees Ins. Co.*, 146 F.3d 1320, 1325 (11th Cir. 1998); *St. Paul Guardian Ins. Co. v. Johnson*, 884 F.2d 881, 884–85 (5th Cir. 1989)).
[246] *See* NCLC FCR § 2.3.5.2 43 (citing 15 U.S.C. § 1681a(d)); *id.* at § 2.3.6.2 47 (citing 2011 FTC Staff Summary § 603(d)(1) Item 7D).
[247] *See* NCLC FCR § 2.3.5.4 45-56 (citing 2011 FTC Staff Summary § 603(d)(1) Item 4 & Item 5c).

reporting purposes is considered a consumer report.[248] Even if the source was ostensibly publicly available information (such as arrests or dispositions of court proceedings), as long as it bears on one of the characteristics protected by FCRA, is provided to a CRA, and is used or expected to be used for a FCRA-related purpose, it is a consumer report covered by FCRA.[249] For example, a CRA reporting the same information contained within a public state Department of Motor Vehicles (DMV) record could constitute a consumer report even though the same record in possession of the DMV might not be covered by FCRA.[250]

As such, the Bureau should also clarify the principle that when data not covered by FCRA is combined with data that is covered by FCRA, both sets of data are now covered by the more protective FCRA.[251] This follows from a similar premise as the algorithm example above —if credit report data is put to other uses, including being combined with non-credit report data, or being used to fuel inferences or other analysis, that renders the entire dataset subject to FCRA. As noted in the recent Energy & Commerce hearing, legal risk mitigation often results in compliance with the lowest standard.[252] The Bureau should explicitly raise the standard.

Both of these points also apply to data clean rooms (DCRs), in which data assets are shared "for specific, mutually agreed upon uses, while guaranteeing enforcement of strict data access limitations."[253] Just as an algorithm built from data that cannot be seen is subject to FCRA,[254] data

[248] *See* NCLC FCR § 2.3.5.4 46 (citing 2011 FTC Staff Summary § 603(d)(1) Item 5c).
[249] *See* 2011 FTC Staff Summary § 603(d)(1) Item 6D.
[250] *See* NCLC FCR § 2.3.4.1.1 37 (citing, *inter alia*, 2011 FTC Staff Summary § 603(d)(1) Item 6D & 6F).
[251] *See* Hoofnagle, *supra* note 168, at 277 ("If these companies [data brokers] merge non-FCRA information with FCRA data, it is all subject to the act"); 2011 FTC Staff Summary § 603(d)(1) Item 4 ("If information from a consumer report is added to a report that is not otherwise a consumer report, that report becomes a consumer report.")
[252] *See* Erwin Testimony at 1.24.10.
[253] IAB Tech Lab, Data Clean Rooms: Guidance and Recommended Practices Version 1.0 10 (Feb. 16, 2023), https://iabtechlab.com/wp-content/uploads/2023/02/FINAL-DRAFT-PUBLIC-COMMENT-Data-Clean-Room-Guidance-IAB-Tech-Lab.pdf [hereinafter "IAB Report"]; *see also* Jon Keegan, *What Are "Data Clean Rooms"?*, Markup (July 1, 2023), https://themarkup.org/hello-world/2023/07/01/what-are-data-clean-rooms.
[254] See discussion of *Heagerty v. Equifax Info. Services LLC, supra* note 244.

enriched through a DCR mechanism would be subject to FCRA if either the appended or the appending data was subject to FCRA. With the deprecation of third party cookies and the increasing use of consumer privacy tools, brands will increasingly be looking for tools like DCRs to power their targeted marketing efforts.[255] This already includes the likes of Disney, Roku, and Kroger.[256] It is important to note that DCRs still present significant privacy risks[257] and are particularly enticing targets by virtue of the volume of data contained within them.[258] Even the IAB, while contending that DCRs provide a measure of privacy and data security, states that the onus is on each DCR user to ensure compliance with all applicable laws,[259] to incorporate privacy controls into contracts, and to perform due diligence and monitoring.[260] We propose Know Your Customer (KYC) protocols further below.

[255] *See, e.g.*, Pamela Parker, *What is Identity Resolution and How are Platforms Adapting to Privacy Changes?*, MarTech (June 1, 2022), https://martech.org/what-is-identity-resolution-and-how-are-platforms-adapting-to-privacy-changes/ (noting that the number of devices connected to IP networks, such as connected speakers, home management solutions, smart TVs, and wearable devices, is expected to more than triple the global population in 2023, citing to Cisco Annual Internet Report, 2018-2023). We note that DCRs is just one method of identity-stitching. Others include (but are not limited to) hashed email, publisher cohorts, universal IDs, and FLOCs. *See, e.g.*, Lore Leitner et al., *Ad Tech: How to Manage Compliance in a New First Party (or NO) Cookie World*, Priv. & Sec. Acad. (Mar. 24, 2022), https://www.privacysecurityacademy.com/ad-tech-how-to-manage-compliance-in-a-new-first-party-or-no-cookie-world/.
[256] *See, e.g.*, James Hercher, *AdExplainer: Data Clean Rooms*, AdExchanger (July 25, 2022), https://www.adexchanger.com/data-exchanges/adexplainer-data-clean-rooms/.
[257] *See, e.g.*, Keegan, *supra* note 253 (citing to IAB best practices guide in listing re-identification attack methods such as "membership inference," "outlier injection," "dictionary," and "manufactured data join" attacks).
[258] *See, e.g.*, *id.* ("Data security also becomes a huge privacy concern when data clean rooms are in control of so much data. Of particular importance is how the data is stored in the clean room. If a breach were to happen, it is critical that the method of data encryption is robust enough to prevent any personal information from being reidentified").
[259] *See* IAB Report at 22 ("While DCRs provide privacy technologies and data governance tools, it is the responsibility of the Data Contributor to ensure that their datasets have the required compliance with applicable privacy regulations (e.g., GDPR, CCPA etc.)").
[260] *See id.* at 24.

Inferences can also be dispositive as to whether a record is a consumer report. Even a dataset containing solely names and addresses could constitute a consumer report if assembled or defined in relation to a characteristic used—even in part—in eligibility decisions.[261]

The definition of a CRA is also relevant to what constitutes a consumer report, as there is a measure of circularity between the definitions. A CRA regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. When an entity "contributes to (or in any way determines the content of) the information conveyed to the client, it is assembling or evaluating" under FCRA.[262] Apps used to screen criminal reports may be CRAs,[263] as could a repository of consumer information from multiple telecom/utility companies (even if each telecom/utility company on its own would not be considered a CRA).[264] Entities that sell data that are aware (or reasonably should know) the reports are being used for credit, insurance, employment, or tenancy screening are CRAs, even if they bind the buyers of their data to non-FCRA uses.[265] In

[261] *See* 2011 FTC Staff Summary § 603(d)(1) Item 6(C)(ii) ("A list of consumers' names and addresses, if assembled or defined by reference to characteristics or other information that is also used (even in part) in eligibility decisions, is a series of consumer reports. For example, a list comprised solely of consumer names and addresses, but compiled based on the criterion that every name on the list has at least one active trade line, updated within six months, is a series of consumer reports.").
[262] NCLC FCR § 2.5.3.2 68.
[263] *See, e.g.*, NCLC FCR § 2.7.1 82 (citing Press Release, FTC, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting-act; Press Release, FTC, FTC Approves Final Order Settling Charges Against Marketers of Criminal Background Screening Reports (May 1, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/05/ftc-approves-final-order-settling-charges-against-marketers-criminal-background-screening-reports).
[264] *See* NCLC FCR § 2.7.11 87 (citing *Heagerty v Equifax Info Services LLC*, *supra* note 244).
[265] *See, e.g.*, Hoofnagle, *supra* note 168, at 277; NCLC FCR § 2.6.3.3 81 (discussing duties of resellers); *id.* at § 2.5.4.3 73 (citing *In re Filiquarian Publishing, L.L.C.*, FTC File No. C-4401 (Apr. 30, 2013) (final decision and order); Letters from Maneesha Mithal, FTC, to Everify, Inc., InfoPay, Inc., and Intelligator, Inc. (Jan. 25, 2012)) (noting mere disclaimers are not enough to absolve FCRA liability); *id.* at § 7.5.1.2 473 n.645 (citing 15 U.S.C. § 1681e(a); *Harrington v ChoicePoint*, Slip Op., No. CV-05-1294 MRP (C.D. Cal. Sept 15, 2005) ("Once the fraudsters indicated they intended to use the information for FCRA purposes it does not matter that in another part of the agreement they promised not to do it… deciding otherwise would allow ChoicePoint to contract around FCRA liability")).

short, the Bureau should clarify that the scope of FCRA is broader than the extent to which it has historically been applied might suggest.

2. Liability attaches when the CRA knew or should have known of an impermissible purpose

An entity has violated FCRA when it knows or reasonably should know that it is releasing reports to users who are without a permissible purpose to access that consumer report.[266] This could include liability for employee misuse of consumer reports if the company did not have adequate safeguards in place to prevent that misuse.[267]

A violation of the "permissible purpose" provision of FCRA also implicates a UDAP violation.[268] The Bureau should be explicit that a FCRA violation also represents a per se UDAAP violation. It also likely implicates a separate violation for the user who supplied a false certification to the CRA about the purpose for which they sought the consumer report (this includes a consumer report initially obtained for a permissible purpose that is later used for an impermissible purpose).[269] The Bureau should make clear to companies that it will pursue enforcement actions where the CRA knew, or had a reason to believe,[270] that a consumer report was being used without a permissible purpose. The Bureau's supervisory authority, discussed further below, may be helpful for investigating trends in how these violations are occurring.

We encourage the Bureau to offer guidance in the form of a non-exhaustive list of multiple, varied, and illustrative examples of impermissible purposes. One category of impermissible purpose is obtaining a credit report in situations in which creditworthiness is no longer relevant—for

[266] *See, e.g.*, NCLC FCR § 2.3.5.2 44 (citing 2011 FTC Staff Summary § 603(d)(1) Item 7C); *see also id.* at § 2.3.5.2 43-44.
[267] *See, e.g.*, NCLC FCR § 7.6 477 (citing 15 U.S.C. § 1681e(a)); *id.* at § 7.7.5 483 (citing 2011 FTC Staff Summary § 607(a) Item 6).
[268] *See* NCLC FCR § 10.6.2 593 (citing 15 U.S.C. § 1681s(a)(1)).
[269] *See* NCLC FCR § 10.2.3.2 575 (citing 15 U.S.C. § 1681b(f), 1681n, 1681o) (obtaining a report for an impermissible purpose is itself a brightline violation of FCRA); *see also id.* at § 14.2.2 817.
[270] *See* NCLC FCR § 7.1.2.2 422 (citing 15 U.S.C. § 1681e(a)).

example, a landlord obtaining a credit report after the tenant has vacated[271] or where creditworthiness was not a relevant factor to renewing their lease[272] or where a credit account was closed and paid in full.[273] Another category is pretextual credit offers, in which the company uses the offer of credit as a ruse to engage in targeted marketing through use of the information contained in a consumer report.[274] A third category is creating accounts or initiating loans without consumer consent.[275] A fourth, second-order category involves the company attempting to preemptively cure its impermissible purpose by obtaining the consumer's signature on an agreement stating that the company "may" access their information, without the consumer affirmatively and explicitly stating that they want their report to be accessed by the company[276] (nor will a signature cure use for an impermissible purpose).[277]

Providing FCRA-covered information to a government agency without a court order is also generally an impermissible purpose. Recall that information obtained for a FCRA-related purpose is covered by FCRA even if the user's interest in that consumer report is not FCRA-related. An administrative subpoena is not sufficient to produce a consumer report to a government agency (except for the IRS,[278] and to a limited extent the FBI[279]). A court order is required for welfare fraud

[271] *See, e.g.*, NCLC FCR § 7.2.8.2.2.3 451.
[272] *See, e.g.*, NCLC FCR § 7.4.11 472 (citing *Ali v. Vikar Mgmt. Ltd.*, 994 F. Supp. 492 (S.D.N.Y. 1998)).
[273] *See, e.g.*, NCLC FCR § 7.4.8 470-71 (citing 2011 FTC Staff Summary §604(a)(3)(A) Item 4).
[274] *See, e.g.*, NCLC FCR § 7.3.3.3.3 461 (citing 2011 FTC Staff Summary § 603(l) Item 5; *Murray v. New Cingular Wireless*, 523 F.3d 719 (7th Cir. 2008); *Cole v. U.S. Capital, Inc.*, 389 F.3d 719 (7th Cir. 2004)) (noting FTC says scrutinize credit in conjunction with sale of goods, to ensure offer is not ruse to obtain consumer report for impermissible purpose).
[275] *See, e.g.*, Consent Order, *In re State Farm Bank, FSB*, 2018-BCFP-0009 at ¶ 17, 19 (Dec. 6, 2018), https://www.consumerfinance.gov/about-us/newsroom/bureau-consumer-financial-protection-settles-state-farm-bank/; Amended Complaint, *CFPB v. Fifth Third Bank, N.A.*, 1:21-cv-262 at ¶ 206 (S.D. Oh. June 16, 2021).
[276] *See* NCLC FCR § 15.5.1 857 (citing 2011 FTC Staff Summary § 604(b)(2) Item 5).
[277] *See* NCLC FCR § 15.5.1 856 (a consumer signature on a document claiming using a credit report for a permissible purpose does not cure use for an impermissible purpose).
[278] *See* 2011 FTC Staff Summary § 604(a)(1) Item 2.
[279] *See* 15 U.S.C. § 1681u.

investigations, criminal or civil prosecutions, and immigration proceedings; to hold otherwise is to permit an end-run around the Constitution's protections under the Fourth Amendment and is a violation of FCRA's permissible purpose provisions.[280] The Bureau should regulate the myriad relationships between government and data brokers.

3. Know Your Customer (KYC) protocols

The Bureau should explicitly require CRAs to undertake ongoing monitoring of users of consumer reports, building upon existing FCRA requirements for due diligence (both in terms of when an individualized certification of permissible purpose is required[281] and in terms of what constitutes an adequate certification).[282] This would help to mitigate downstream misuses of consumer reports. It would be consistent with the IAB's best practice guidance,[283] and would also be consistent with proposed legislation in Congress.[284] Again, the Bureau's supervisory authority can be helpful for assessing and enforcing compliance here.

[280] *See, e.g.*, NCLC FCR § 7.4.5 467 (citing to multiple FTC staff letters).
[281] *See* NCLC FCR § 7.5.2.2 474 (citing 2011 FTC Staff Summary § 607(a) Item 4B) (noting that if a user (e.g., a detective, attorney, or insurance company) is likely to have permissible and impermissible purposes, each usage must be accompanied by certification, no blanket certification is allowed).
[282] *See* 2011 FTC Staff Summary § 607(a) Item 3 ("[W]hat constitutes adequate certification will vary with the circumstances. Appropriate procedures might require an on-site visit to the user's place of business, a check of the user's references, confirmation of the business identity of the applicant (e.g., via phone directories or publicly available data such as governmental licensing information), and examining applications and supporting documentation supplied by applicants, or other reasonable methods, to detect suspect representations, discrepancies, illogical information, suspicious patterns, factual anomalies, and other indicia of unreliability").
[283] *See* IAB Report at 24.
[284] *See, e.g.*, Consumer Online Privacy Rights Act (COPRA), S.2968, 116th Cong. § 203(c)(1)(a) (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968/text (requiring that covered entity "exercise reasonable due diligence in selecting a service provider and conduct reasonable oversight of its service providers to ensure compliance with the applicable requirements of this section"); *id.* § 203(c)(1)(b) (requiring that covered entity "exercise reasonable due diligence in deciding to transfer covered data to a third party, and conduct oversight of third parties to which it transfers data to ensure compliance with the applicable requirements of this subsection."); ADPPA § 302(e)(1) (requiring that covered entity or service provider "shall exercise reasonable due diligence in—(A) selecting a service provider; and (B) deciding to transfer covered data to a third party.").

4. FCRA's procedures are essential to Congress' intended balancing of interests

The Bureau should be clear that while any single FCRA requirement may seem "merely" procedural or technical, collectively these consumer rights (e.g., awareness of what data is held about them and is being used to make decisions about them, the ability to correct that data, etc.) reflect the intent of Congress to balance the intricate problems involved in the use of consumer records.[285] If entities want to be exempt from tort liability, they must comply with all of the requirements Congress set forth to ensure that consumers have a meaningful way to exercise their rights. The Bureau should consider how it can use its authority under FCRA, as well as its UDAAP authority, to prevent companies from impeding a consumer's awareness of or ability to exercise their rights under FCRA.

ii. Other Recommendations

The below suggestions may, but do not necessarily, require a more formal rulemaking process for the Bureau to successfully implement them. This set of FCRA-related recommendations covers (1) presuming data brokers to be CRAs; (2) data security; (3) risk mitigation companies (e.g., fraud detection and ID verification); (4) alternative credit data; (5) tenant screening; (6) pre-conviction data; and (7) targeted marketing.

1. Data brokers are presumptively CRAs

As discussed above, we urge the Bureau to treat all data brokers presumptively as CRAs, unless the broker demonstrates ongoing, effective efforts to prevent the data they traffic in from being used for any of FCRA's enumerated purposes. FCRA enjoys broad applicability. Due to the propensity for downstream misuse of data, the lack of vetting performed by brokers, and the lack of transparency to both consumers and enforcement entities about whether misuse is occurring, it is

[285] *See, e.g.*, Hoofnagle, *supra* note 168, at 287 (e.g., running reports on old version of public record).

appropriate for the Bureau to establish that a data broker who does not take adequate affirmative steps to prevent its data from being used for FCRA purposes is subject to FCRA.

2. FCRA promotes data security through provisions on impermissible purpose and secure disposal

We urge the Bureau to modernize FCRA to meet the data security challenges of the present day;[286] we believe it can do that by being explicit about liability for inadvertent and unauthorized disclosures and by incorporating the principle of data minimization into its regulations surrounding secure disposal of data. The Bureau might look to the FTC's recent proposal to update its Health Breach Notification Rule as a model, which incorporates health apps and similar technology not covered by HIPAA, considers unauthorized disclosures to be a "breach of security," and expands upon the content required in a breach notification to consumers.[287]

[286] *See, e.g.*, Krebs et al., *supra* note 229; *see also Record Number of Data Breaches in 2021*, IAPP Daily Dashboard (Jan. 25, 2022), https://iapp.org/news/a/record-number-of-data-breaches-in-2021/ (citing to ITRC report which estimated "1,862 breaches last year, up 68% from the year prior, and exceeded 2017's previous record of 1,506"); EPIC Commercial Surveillance FTC Comments at 182 n.835; Brian Krebs, *Identity Thieves Bypassed Experian Security to View Credit Reports*, KrebsonSecurity (Jan. 9, 2023), https://krebsonsecurity.com/2023/01/identity-thieves-bypassed-experian-security-to-view-credit-reports/; Graham Cluley, *Hackers Demand $15 Million Ransom from TransUnion After Cracking "Password" Password*, Bitdefender (Mar. 21, 2022), https://www.bitdefender.com/blog/hotforsecurity/hackers-demand-15-million-ransom-from-transunion-after-cracking-password-password/; Justin Sherman, *Data Brokers and Data Breaches*, Duke Sanford Sch. Pub. Pol'y Blog (Sept. 27, 2022), https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/. The FTC has alleged inadequate security as FCRA violations numerous times. *See, e.g.*, Complaint, *In re Fajilan and Associates, Inc.*, FTC File No. 923089 ¶ 15 (Aug. 19, 2011), https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3089-fajilan-associates-inc-also-dba-statewide-credit-services-matter; Complaint, *In re ACRAnet, Inc.*, FTC File No. 923088 ¶ 13 (Aug. 19, 2011), https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3088-acranet-inc-matter; Complaint, *In re SettlementOne Credit Corporation*, FTC File No. 823208 ¶ 15 (Aug. 19, 2011), https://www.ftc.gov/legal-library/browse/cases-proceedings/082-3208-settlementone-credit-corporation; Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

[287] *See* Press Release, FTC, FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule (May 18 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule.

It is a violation of FCRA's permissible purpose provision to "furnish" by allowing data to be accessed by hackers or by failing to prevent unauthorized access by entities who might otherwise have (or who may have formerly had) a permissible purpose to access the consumer reports. This is part of the reason why the KYC protocols we recommend above are so important. The CRA must have had reasonable and effective procedures to limit unauthorized access to the consumer reports, which notably includes changing its methods if it learns that someone obtained unauthorized access.[288] CRAs are liable both for negligent or willful disclosures without a permissible purpose **and** for a negligent or willful failure to maintain reasonable procedures designed to limit furnishing consumer reports to entities with a permissible purpose.[289] Blanket certifications do not excuse CRAs from their obligations to verify that consumer reports are being used for impermissible purposes, especially if there is reasonable ground to suspect impermissible use.[290] Similarly, CRAs must have procedures in place to ensure consumer consent to have their consumer report accessed is genuine,[291] and to deny access to creditors once a credit is paid in full and the account is closed.[292] Failure to maintain any of these procedures should constitute a per se violation of FCRA. The Bureau should

[288] *See* 2011 FTC Staff Summary § 607(a) Item 6 (CRA must have reasonable and effective procedures to limit unauthorized access to its databases….if it appears that a person has obtained unauthorized access to a CRA's computerized files, the CRA must take appropriate steps including altering the means of access, such as changing codes and passwords, and making random checks to verify that reports are obtained only for permissible purposes); NCLC FCR § 7.2.8.2.4 452 (citing *Rand v Citibank*, 2015 WL 510967 (N.D. Cal. Feb. 6, 2016)) (identity theft excuses pulling report for non-consumer if defendant did not know it was fraud, but impermissible if defendant knew, e.g., wrong SSN used).
[289] *See* NCLC FCR § 7.5.1.1 472 (citing 15 U.S.C. § 1681b, 1681n, 1681o, 1681e(a)) (CRA is liable for negligent or willful disclosure without permissible purpose OR for negligent or willful failure to maintain reasonable procedures to limit furnishing of consumer reports to permissible purposes); *see also* 2011 FTC Staff Summary § 607(a).
[290] *See* NCLC FCR § 7.5.2.2 474 (citing to 2011 FTC Staff Summary § 607(a) Item 4B) (noting that if a user (e.g., a detective, attorney, or insurance company) is likely to have permissible and impermissible purposes, each usage must be accompanied by certification, no blanket certification is allowed).
[291] *See* 2011 FTC Staff Summary § 607(a) Item 8.
[292] *See* NCLC FCR § 7.5.2.3 475 (citing 2011 FTC Staff Summary § 607(a) Item 7).

make explicit that a procedure is presumptively unreasonable if it results in an unauthorized disclosure.

The Bureau should also work with the FTC to incorporate principles of data minimization into its rules for secure disposal of data.[293] We believe this can be achieved by amending the definition of "abandoned" files to include stale, digitally-stored data.[294] While digitally-stored data is less visible than stacks of files in a room, office, or dumpster,[295] it is no less sensitive (and may actually be more vulnerable to misuse). The Bureau should amend the definition of "abandoned" in 16 C.F.R. § 682 to include information that is "no longer strictly necessary for business purposes."

As we note above, consumers are in no position to detect when a breach has occurred; their injuries may be delayed if bad actors do not immediately attempt to use the breached data; and consumers may suffer multiple, distinct injuries at the hands of various fraudsters over the course of several months or years as a result of single breach. The Bureau should work with its sister agencies to mitigate these harms by incentivizing stronger data security practices.

3. Fraud detection/ID verification companies are CRAs

We urge the Bureau to treat fraud detection, ID verification, and similar companies as CRAs,[296] chiefly for two reasons. First, there is no discernible difference to the consumer whether they were denied an opportunity due to a fraud flag or due to being ineligible for other reasons. (This is related to issues of downstream misuse of consumer reports as well, as accountability for

[293] *See* Hoofnagle, *supra* note 168, at 285 ("The FTC retains authority over…§1681w, dealing with disposal of consumer report information").
[294] 16 C.F.R. § 682.1(c)(1).
[295] *See, e.g.*, *FTC v. PLS Financial Services, Inc.*, FTC File No. 1023172 (Nov. 7, 2012), https://www.ftc.gov/legal-library/browse/cases-proceedings/1023172-pls-financial-services-inc-et-al; *FTC v. Gregory Navone*, FTC File No. 723067 (Jan. 20, 2010), https://www.ftc.gov/legal-library/browse/cases-proceedings/072-3067-navone-gregory; *FTC v. American United Mortgage Company*, FTC File No. 623103 (Dec. 18, 2007), https://www.ftc.gov/legal-library/browse/cases-proceedings/062-3103-american-united-mortgage-company-united-states-america-ftc.
[296] *See, e.g.*, NCLC FCR § 2.7.12 88 ([databases providing fraud risk scores] appear to meet the definition of CRAs).

preventing misuse of reports is difficult without being able to determine why an individual was denied a credit, housing, or job opportunity.) Second, if fraud detection/ID verification companies are using inaccurate information to deny consumers services, consumers should be able to access and correct that inaccurate information. This presents logistical challenges, as we do not want to permit fraudsters to define the keys necessary to obtain access to a victim's data,[297] but the alternative is to continue leaving consumers underserved and in the dark about why they are being denied. A rulemaking could be an effective vehicle for navigating the equities on either side.

FCRA defines a consumer report, in part, as any communication bearing on a consumer's character or general reputation used or collected for the purpose of serving as a factor in establishing the consumer's eligibility for credit, employment, or similar purposes.[298] By providing identity verification services, companies providing fraud detection, ID authentication, and similar services effectively determine whether any single applicant falls above or below a certain trust threshold, which in turn determines their eligibility for credit, insurance, and employment offerings. If a fraud detection, ID authentication, or similar company markets its services to employers, recruiters, companies operating in the credit industry, and similar entities—or if there are other reasons to expect it will use the consumer data it has to determine a consumer's suitability for FCRA-covered activities—then the information it collects to provide its services is collected for FCRA-covered purposes. This is true even if that information is ultimately used in other contexts (e.g., fraud detection in a public benefits context).

[297] Several examples are provided by Krebs, *supra* note 229. This is akin to SIM swapping, when a fraudster takes control of a victim's phone enabling them to intercept multi-factor authentication messages with the end goal of compromising more sensitive financial accounts. *See, e.g.*, Jon Brodkin, *Man Sues AT&T After Fraudulent SIM Led to $1.8M Cryptocurrency Theft*, Ars Technica (Oct. 24, 2019), https://arstechnica.com/tech-policy/2019/10/att-employees-helped-sim-swap-hackers-rob-man-of-1-8-million-lawsuit-says/.
[298] 15 U.S.C. § 1681a(d)(1).

The Bureau should determine that, because fraud detection, ID authentication, and similar companies insert themselves as gatekeepers between consumers and FCRA-related opportunities on the basis of a consumer's trustworthiness, these companies are acting as CRAs insofar as they (1) regularly engage in the practice of assembling information on consumers for the purpose of furnishing consumer reports to third parties or (2) determine the content of information conveyed to the clients of consumer reports. Further, as argued above, any report derived, at least in part, from FCRA-covered data should itself be covered by FCRA. For instance, a report noting that an application was denied for reasons related to fraud or to failed identity authentication should be covered by FCRA.

We acknowledge that historically the FTC has distinguished fraud detection from credit reporting;[299] however, for the reasons listed above the Bureau should change this classification. This kind of reversal is not entirely unprecedented, as in 2011 the FTC reversed its own position on whether coded lists were subject to FCRA in recognition of changes in technology.[300]

4. Protections for alternative data

The Bureau should implement protections for individuals without credit scores or who otherwise rely upon alternative data to obtain credit.[301] Notably, the FTC has pursued FCRA

[299] *See, e.g.*, FTC Data Brokers Report at i (2014) (citing FTC, Protecting Consumer Privacy in an Era of Rapid Change 65 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf); *see also id.* at 20–21 (noting that "a communication that flags a specific Internet transaction as potentially fraudulent based on comparison to aggregate data about Internet transactions (e.g., time-of-day activity, geographic location, amount of the transaction, etc." is not a credit report, but would be a CR if it could otherwise reasonably be linked to the consumer "even if it does not identify the consumer by name").
[300] *See* 2011 FTC Staff Summary at 11.
[301] NCLC discusses encouraging uses of alternative credit data as well as harmful ones. *See, e.g.*, Chi Chi Wu, *Credit Invisibility and Alternative Data: Promises and Perils*, NCLC (July 1, 2019), https://www.nclc.org/resources/credit-invisibility-and-alternative-data-promises-and-perils/; Chi Chi Wu & Carolyn Carter, *No Silver Bullet: Using Alternative Data for Financial Inclusion and Racial Justice*, NCLC (June 1, 2022), https://www.nclc.org/resources/no-silver-bullet-using-alternative-data-for-financial-inclusion-and-racial-justice/.

violations against apps that draw upon stored consumer information from sources outside the consumer's direct interaction with the app.[302] In 2016, the FTC noted that even data not traditionally associated with creditworthiness (e.g., ZIP code, social media usage, shopping history) can be subject to FCRA if that data is used or expected to be used to determine a consumer's suitability for credit, employment, insurance, housing, or other similar benefits and transactions.[303] In at least one instance, a credit issuer has included capitalization of the applicant's name in their application as a risk factor.[304] Even seemingly innocuous data may be used for FCRA-covered purposes.

FCRA likely would not apply where these companies only share data based on their own transactions with the consumer (e.g., payment history);[305] however, if any information is collected from a secondary source (e.g., social media contacts) to determine the consumer's risk level, that company's record should be treated as a consumer report if shared (or expected to be shared) with a third party.

5. Ban use of credit reports in tenant screening

The Bureau should ban the use of credit reports in tenant screening.[306] As NCLC has articulated, credit reports do not predict current ability to pay, are riddled with errors, and perpetuate

[302] *See, e.g.*, Press Release, FTC, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting-act.
[303] *See, e.g.*, FTC, Big Data: A Tool for Inclusion or Exclusion? ii (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.
[304] *See* Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J.L. & Tech. 148, 164 n.74 (2016) (citing Michael Carney, *Flush with $20M from Peter Thiel, ZestFinance is Measuring Credit Risk Through Non-traditional Big Data*, Pando (July 31, 2013), https://perma.cc/PZ5R-WPJG ("Merrill [ZestFinance CEO] explains… that the way a consumer types their name in the credit application – using all lowercase, all uppercase, or correct case – can be a predictor of credit risk.")).
[305] See discussion of first party data and third party data above.
[306] *See generally* Chi Chi Wu, *Even the Catch-22s Come With Catch-22s: Potential Harms & Drawbacks of Rent Reporting*, NCLC (Oct. 24, 2022), https://www.nclc.org/resources/even-the-catch-22s-come-with-catch-22s-potential-harms-drawbacks-of-rent-reporting/ (rent payment data is new trove of info but it will be used at expense of vulnerable renters); NCLC, Comments on Tenant Screening Request for Information by FTC and CFPB (May 30, 2023), https://www.nclc.org/resources/comments-on-tenant-screening-request-for-

inequalities and injustices.[307] EPIC recommends the Bureau consult NCLC's excellent resource on this topic, *2023 Consumer Reform Priorities to Protect Tenants*.[308]

6. Ban use of pre-conviction data in credit reports

The Bureau should also ban use of pre-conviction criminal proceeding information in credit reports.[309] For example, at the arrest stage there has not yet been a determination of innocence or guilt, and there is ample evidence to suggest that arrest statistics are influenced by racial bias.[310] There is also evidence that consumer reports often fail to reflect the most updated disposition of a proceeding, meaning someone arrested or charged but determined to have been not guilty by a jury might still be subject to the stigma of criminal proceeding information in their consumer report.[311] This is similar to the failure to update eviction information to reflect that the judgment has been satisfied.[312]

---

information-by-ftc-and-cfpb/; Chi Chi Wu & Michael Best, *Why We Need the Fair Chance in Housing Act (FCHA) to Keep Credit Reports Out of Housing Decisions Now*, NCLC (Mar. 15, 2023), https://www.nclc.org/resources/why-we-need-the-fair-chance-inhousing/.

[307] *See, e.g.*, Fact Sheet, *An Act Relative to the Use of Credit Reporting in Housing H1429/S894, the Fair Chance in Housing Act: Senator Lesser, Representative Malia*, NCLC, https://www.nclc.org/wp-content/uploads/2022/09/MA_Credit_Housing.pdf (last visited July 12, 2023).

[308] NCLC, 2023 Consumer Reform Priorities to Protect Tenants (2023), https://www.nclc.org/resources/2023-consumer-reform-priorities-to-protect-tenants/ (calling for prohibition on evictions (or at least those not resulting in judgments), sealed/expunged records, debt arising from COVID, convictions 7+ years old, non-conviction criminal records 4+ years old, also calling for extending notices and requirements for employment uses to tenant/housing uses, routinely testing scores and recommendations, providing specific reasons for denying housing).

[309] *See, e.g.*, Hoofnagle, *supra* note 168, at 288–89 (urging regulators to not allow arrest info to remain in records for seven years).

[310] *See, e.g.*, Magnus Loftstrom et al., Prison Pol'y Inst. Cal., Racial Disparities in Law Enforcement Stops (2021), https://www.ppic.org/publication/racial-disparities-in-law-enforcement-stops/; The Sentencing Project, Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System (2018), https://www.sentencingproject.org/reports/report-to-the-united-nations-on-racial-disparities-in-the-u-s-criminal-justice-system/; U.S. Gov't Accountability Off., GGD-94-29R, Racial Differences in Arrests (1994), https://www.gao.gov/products/ggd-94-29r.

[311] *See, e.g.*, OSF Data Brokers Report at ; Oyama *supra* note 177.

[312] Similar but not identical, as a monetary judgment has direct credit/debt-related impact whereas incarceration has more indirect implications.

7. Blurred lines with marketing

The Bureau should also re-evaluate the extent to which the data used in targeted marketing programs implicates credit evaluations and/or risk-based pricing. The line between marketing and credit offers is not entirely clear.[313] Risk scores may be used to generate leads to serve ads that are not formal pre-approved offers of credit.[314] As Ed Mierzwinski and Jeff Chester have noted:

> [T]he challenge for policymakers at the FTC and the [CFPB] will be to evaluate the new landscape and determine answers to the following questions… At what point does an Internet profile or consumer dossier containing information bearing on any one of the FCRA's seven factors, from creditworthiness to mode of living, make a profile into a consumer report . . . When does a decision derived from a profile acquired through serving an ad tied to a financial offer become an offer based on a decision affecting a consumer's eligibility for credit, insurance, or employment? . . . When does a decision selecting some consumers for different higher or lower cost, or more or less desirable products, become an "adverse action" or a "risk-based pricing" selection subject to the FCRA? . . . Where is the line between a score calculated simply to serve a targeted ad and a score used to determine a consumer's eligibility for credit?[315]

---

[313] *See, e.g.*, Hoofnagle, *supra* note 168, at 285 ("The FCRA does not apply to marketing generally, but, at the same time, the line between marketing and credit offers is not entirely clear. A website might screen a consumer in its marketing efforts and show ads for different financial products."); WPF Report at 11 ("Oddly, direct marketing lists and activities have the potential to strike deeply into the lives of individuals in quirky ways that can have an impact on consumer lifestyle. Much remains to be learned about the impact of consumer scoring in the direct marketing arena, as well as eligibility issues and edge-eligibility issues like scores for identity and authentication."); Ed Mierzwinski & Jeff Chester, *Selling Consumers Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act*, 46 Suffolk U. L. Rev. 845, 846 (2013) ("The interplay of traditional CRAs, lenders, online data brokers, and interactive digital financial advertisers has blurred the line between the traditional definitions of CRAs and target marketing. The emergence of instantaneous online consumer-credit evaluations, which use traditional and new forms of scoring, coupled with an explosion of Internet-based profiling and lead-generation techniques, requires regulators and advocates to closely examine this new consumer landscape."); *id.* at 858 ("Lead lists appear to be no different from prescreened lists marketed for the intention of selling credit offers"); *id.* at 868 ("The murky and purposefully ill-defined divisions among online lead generation, consumer profiling, scoring, and tracking, coupled with the integration of advertising and direct sales, have created new challenges for both consumers and regulators.").

[314] *See, e.g.*, WPF Report at 43 n.63 (citing *Spring Privacy Series: Alternative Scoring Products*, FTC (Mar. 19, 2014), http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products). ("Sending an advertisement to a consumer is not the same thing as sending a formal, pre-approved offer of credit as described in the FCRA. This risk score category includes risk scores that may well be used to generate leads, but the advertisements themselves are not formal pre-approved offers of credit.").

[315] Mierzwinski & Chester, *supra* note 313, at 861–62, 879 ("…a key threshold question for regulators is determining when information is used merely to target ads, and when it is used to establish eligibility for credit or other actions that would bring their practices under the FCRA. The CFPB and FTC should also examine the merging of online and offline data used for both scoring and targeting individual consumers. A

FCRA prohibits the use of consumer reports for targeted marketing,[316] except where used for prescreened firm offers of credit.[317] Yet companies offer lead-generation products seemingly based on credit report information.[318] Indeed, ads served based on creditworthiness information should render the practice actionable under FCRA.[319]

Credit offered on less favorable terms constitutes risk-based pricing and requires an adverse action disclosure.[320] The Bureau should construe "credit" broadly to include mechanisms such as earned waged advances,[321] as well as services for which the user is billed after service or product is

---

full inquiry into how financial-services companies are using online marketing to profile and target individual consumers is required…The CFPB and FTC should ensure that consumers know whether (and how) they have been secretly scored or rated by digital financial marketers, especially those consumers labeled as less profitable or undesirable. The new breed of online data-warehousing companies that sell access to consumers' financial behavior, and those that are part of the digital targeting chain, also require scrutiny.").

[316] *See, e.g.*, *id.* at 854 (citing *In re Trans Union Corp.*,FTC File No. 9255, 2000 WL 257766, at *12 (Feb. 10, 2000)) (describing FTC action against TransUnion) ("In reaching this conclusion, we examined Trans Union's various target marketing lists--the Master File/Selects, proprietary models, and reverse append products--and find that information disclosed through these products is the type of information that is "used" and/or "expected to be used" in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for credit. Accordingly, these products are consumer reports and Trans Union cannot lawfully sell them for target marketing purposes[[.]").

[317] *See, e.g.*, Hoofnagle, *supra* note 168, at 277 (citing Press Release, FTC, Consumer Reporting Agency to Pay $1.8 Million for Fair Credit Reporting Act Violations (June 27, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/06/consumer-reporting-agency-pay-18-million-fair-credit-reporting-act-violations); 2011 FTC Staff Summary § 604(a) Item 6B (sellers of goods and services do not have a permissible purpose to obtain consumer reports for marketing purposes, but they can make firm offers of credit).

[318] *See* Mierzwinski & Chester *supra* note 313, at 858 ("Equifax offers a variety of twenty-first-century lead-generation products based on credit reports, including TargetPoint Cross-Sell: 'Utilizing your target marketing list or customer database file, matched against Equifax's industry leading credit marketing database, Equifax identifies consumers within your portfolio who have recently demonstrated interest in obtaining additional credit.'").

[319] *See, e.g.*, *id.* at 876 ("When an online score is linked to a cookie and multiple sources of offline and online information, it becomes a powerful screening and consumer-credit-assessment system. Triggering an offer based on creditworthiness information could render these practices actionable under the FCRA.").

[320] *See, e.g.*, NCLC FCR § 2.7.13 88 (if the info is used not only to market to the consumer but also to evaluate the consumer's creditworthiness and to determine whether the consumer qualifies and at what price, then it should be viewed as a CRA, and use in marketing likely violates FCRA unless prescreening rules are followed. If company assesses creditworthiness and determines price consumer would pay if consumer responds to offer, that should be considered CR subject to FCRA even if marketing use of report is impermissible); *id.* § 19.2.1.4 573 (citing 15 U.S.C. § 1681m(h)(1)) (discussing risk-based pricing notice).

[321] *See* NCLC, Earned Wage Advances and Other Fintech Payday Loans: Workers Shouldn't Pay to be Paid (2023), https://www.nclc.org/resources/earned-wage-advances-and-other-fintech-payday-loans-workers-shouldnt-pay-to-be-paid/.

provided, such as phone or internet service.[322] The Bureau should also consider how FCRA's fairness guidelines might apply to comparison shopping and/or dynamic pricing.[323]

While a company using its own customer data to make internal credit determinations would not be treated as a CRA for that reason alone (first-party data),[324] a company selling an algorithm or providing analytics services to clients (third-party data, from the client's perspective) to make eligibility determinations based on the analytics company's data should be treated as a CRA, and both the company and its clients should be subject to FCRA.[325]

Even seemingly generic information should not get a pass by default. Some may argue that sharing consumer lists built from generic data does not constitute a FCRA violation.[326] However, it can be difficult to determine whether that generic information has been coupled with or filtered by covered information pertaining to creditworthiness, such as information indicating that an individual was denied credit; use of proxies for this data, such as a cell phone turndown list, may further obscure this reality.[327] The Bureau should explore how a rulemaking could support future enforcement actions against entities that circumvent FCRA by using proxies for FCRA-covered data,

---

[322] *See* NCLC FCR § 7.2.3.4.2 440) (citing *Phox v NCO Fin. Sys.*, 2014 WL 5438381 (W.D. Mo. Oct. 24, 2014)) (internet service bills could be considered credit, as service isn't terminated if bill paid one day late, and bill is sent after services are provided, courts may be inclined to consider debt collection activities that for years used CRs as credit).

[323] *See, e.g.*, Hoofnagle, *supra* note 168, at 288.

[324] *See, e.g.*, Terrell McSweeny, *FTC 2.0: Keeping Pace with Online Platforms*, 32 Berkeley Tech. L.J. 1027, 1045–46 (2017) (citing 15 U.S.C. § 1681a(d)(2)(A)(i)) (exempting "report[s] containing information solely [gained from] transactions or experiences between the consumer and the person making the report"); Hurley & Adebayo, *supra* note 304, at 187 (citing to same provision of 1681) ("For example, a lender that develops its own mechanisms for collection and data analytics will not trigger FCRA as long as it does not resell that information for further use in the credit, insurance, or employment context"); NCLC FCR § 2.7.13 88 (not CR if info collected through company's own reward program, or through affiliate unless consumer opted out).

[325] *See* McSweeny, *supra* note 324, at 1045–46 (citing FTC, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues 15 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf).

[326] *See, e.g.*, NCLC FCR § 7.3.2.2 456-57; *id.* at § 7.3.2 456-57.

[327] *See, e.g.*, WPF Report at 59 (describing a list of individuals denied a cell phone, which could serve as a proxy for low credit); *id.* at 43 (writing in 2014 that "[m]odern data analytics have made child's play of unearthing people who are in various credit score brackets without revealing the actual credit score."); FTC Data Brokers Report at iv–v, 20, 47 (noting "Urban Scramble" and "Mobile Mixers" categories).

especially in the context of lead generation and targeted marketing, and especially as it relates to vulnerable populations.

c. The Consumer Financial Protection Act

Regardless of whether FCRA applies to a given practice or not,[328] the Bureau has authority under the CFPA to prevent deceptive, unfair, or abusive acts or practices in connection with any transaction with a consumer for a consumer financial product or service ("consumer financial product") or with the offering of a consumer financial product, and to detect and assess risks to consumers and to markets for consumer financial products.[329] What constitutes a deceptive and/or unfair act or practice has been well established through the enforcement work of the Bureau, the FTC, and state attorneys general. And earlier this year, the Bureau issued a policy statement on abusive acts or practices, which it summarized as "(1) obscuring important features of a product or service, or (2) leveraging certain circumstances to take an unreasonable advantage."[330]

Using its authority under the CFPA, the Bureau should (1) ban secret scoring; (2) require creators of scoring systems to demonstrate that their scores cannot be used in a way that supports

---

[328] *See* NCLC FCR § 10.6.2 593 (citing 15 U.S.C. § 1681s(a)(1)).

[329] *See* Press Release, CFPB, CFPB Warns that Digital Marketing Providers Must Comply with Federal Consumer Finance Protections (Aug. 10, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-that-digital-marketing-providers-must-comply-with-federal-consumer-finance-protections/ ("Digital marketers, on the other hand, seek to maximize individuals' interactions with ads. They may harvest personal data to feed their behavioral analytics models that can target individuals or groups that they predict are more likely to interact with an ad or sign up for a product or service. When digital marketing providers go beyond traditional advertising, they are typically covered by the Consumer Financial Protection Act as service providers"); *Unfair, Deceptive, or Abusive Acts or Practices (UDAAPs) Examination Procedures*, CFPB (Mar. 16, 2022), https://www.consumerfinance.gov/compliance/supervision-examinations/unfair-deceptive-or-abusive-acts-or-practices-udaaps-examination-procedures/; Press Release, CFPB, CFPB Targets Unfair Discrimination in Consumer Finance (Mar. 16, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-targets-unfair-discrimination-in-consumer-finance/ ("CFPB examiners will require supervised companies to show their processes for assessing risks and discriminatory outcomes, including documentation of customer demographics and the impact of products and fees on different demographic groups").

[330] *Policy Statement on Abusive Acts or Practices*, CFPB (Apr. 3, 2023), https://www.consumerfinance.gov/compliance/supervisory-guidance/policy-statement-on-abusiveness/ [hereinafter "Abusiveness Policy Statement"] (supervisory guidance).

invidious discrimination; (3) mandate reporting on the quality of data factors used in scoring; (4) ban the disclosure and purchase of sensitive data; (5) regulate neighborhood-level data; (6) prevent discrimination in targeted marketing; (7) regulate fraud scoring; (8) prohibit disclosure and purchasing of pre-conviction data; (9) create additional protections for use of alternative credit data; and (10) account for changes in technology.

In addition to its rulemaking and enforcement authorities under FCRA and CFPA, the Bureau has supervisory authority over nonbank entities that act as larger market participants. We separately address the Bureau's abusiveness authority and its supervisory authority over larger market participants in the credit reporting industry.

i. Specific recommendations for applying the CFPA to data brokers

1. Ban secret scoring

For data products that do not constitute consumer reports under FCRA, the Bureau should mandate public disclosure of consumer scoring. Secret consumer scores are an inherently unfair and deceptive trade practice.[331] Secret scores preclude rights of access, correction, and opting out. This includes shadow profiles (discussed above) that include scores. The Bureau should require that any entities subject to its authority under the CFPA provide free access and correction rights, or else families may be forced to pay an exorbitant sum for each member of their family to each data broker performing any form of scoring.[332]

2. Require score creators to demonstrate scores cannot support invidious discrimination

Relatedly, the creators of scores should state publicly the purpose, composition, and uses of their scores. These disclosures would be subject to Bureau enforcement actions if the public

[331] *See, e.g.*, Citron & Pasquale, *supra* note 7, at 31 ("To be sure, it is impossible to challenge a scoring system that consumers do not even know exists. Secret scores about people's health, employability, habits, and the like may amount to unfair practices even though they fall outside the requirements of FCRA.").
[332] *See, e.g.*, WPF Report at 25.

statements were deceptive, unfair, or abusive. The Bureau should additionally require that any entities subject to its authority under the CFPA that are creators of consumer scoring tools (used internally and/or offered as products or services to client firms) demonstrate that their scores cannot be used to support invidious discrimination.[333] This is consistent with FTC policy.[334] The Bureau could invoke its supervisory authority to achieve this if necessary.[335]

3. Mandate reporting on quality of data factors used in scoring

The quality of data used to make decisions about consumers, even non-credit-related decisions, should be transparent. This is especially important as FCRA-covered data is notoriously inaccurate and difficult for consumers to correct;[336] data that is not subject to FCRA's protections is likely even less accurate. The Bureau should require entities subject to its authority to assess and report periodically on the quality of the data they use in scoring consumers. This includes social media data or inferences made from social media data.[337]

---

[333] *See, e.g.*, WPF Report at 13, 25 (referencing ECOA).

[334] *See, e.g.*, Rohit Chopra et al., Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems *(*Apr. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf; Michael Atleson, FTC, Combatting Online Harms Through Innovation 6–9, 52 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf; Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC Bus. Blog (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai; Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC Bus. Blog (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms;*cf. also* Rebecca Kelly Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 Yale J.L. & Tech. 1, 13–14, 20–24, 35 n.104 (2021).

[335] See Larger Market Participant section below.

[336] *See, e.g.*, Press Release, CFPB, CFPB Issues Report on TransUnion, Experian, and Equifax (Jan. 3, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-report-on-transunion-experian-and-equifax/.

[337] Notably, social media data in some contexts will already be covered by FCRA. *See, e.g.*, Pauline T. Kim & Erika Hanson, *People Analytics and the Regulation of Information Under the Fair Credit Reporting Act*, 61 St. Louis U. L.J. 17, 30 (2016) (citing Lesley Fair, *The Fair Credit Reporting Act & Social Media: What Businesses Should Know*, FTC Bus. Blog (June 23, 2011), https://www.ftc.gov/business-guidance/blog/2011/06/fair-credit-reporting-act-social-media-what-businesses-should-know); WPF Report at 26.

4. Ban disclosure and purchase of sensitive data

The Bureau should treat sharing sensitive categories of data—such as data about health and geolocation—with third parties as presumptively harmful to consumers due to the risks of stalking and vigilantism,[338] and their disclosure and purchase should be prohibited. Even purportedly deidentified data can be reidentified through device ID, browser fingerprinting, and/or correlation with other datasets.

Additionally, the Bureau should closely examine secondary uses of sensitive data within the organization collecting the data. Data that is unobjectionable in one context may be inappropriate in others,[339] and secondary uses even within the same organization should not be presumed to be in consumers' best interests.

The Bureau should also require entities subject to its authority to adequately secure sensitive data.[340]

5. Regulate neighborhood-level data

FCRA only applies to data reasonably linkable to an individual. This means that data pertaining to a neighborhood, household, or IP address or device ID used by multiple individuals could fall outside the scope of FCRA,[341] if it is not reasonably linkable to an individual.[342] This is true even if microtargeting to a 'neighborhood' of seven households.[343] As one salesman in the insurance space "joked" about the potential for error in applying regional-level data to individuals:

[338] *See, e.g.*, Sherman Testimony at 58.07.
[339] *See, e.g.*, WPF Report at 16.
[340] *See, e.g.*, EPIC Commercial Surveillance FTC Comments at 204–05.
[341] *See* Hurley & Adebayo, *supra* note 304, at 184 (2016); WPF Report at 46.
[342] *See* 2011 FTC Staff Summary at 11 ("information may constitute a consumer report even if it does not identify the consumer by name if it could 'otherwise reasonably be linked to the consumer'").
[343] *See* Mierzwinski & Chester, *supra* note 313, at 870.

"God forbid you live on the wrong street these days. . . . You're going to get lumped in with a lot of bad things."[344]

To the extent household- or device-level data is linkable to an individual, it should be treated as FCRA-covered data. To the extent it is not, and for neighborhood-level data and similar types of data, the Bureau should utilize its authority under the CFPA to protect consumers from adverse determinations being made about them due to circumstances that may have nothing to do with them (i.e., "get[ting] lumped in with a lot of bad things").

Additionally, there may be reidentification risks, such as when data that was not linkable to an individual when it was shared with a third party is subsequently relinked to that individual.[345]

6. Prevent discrimination in targeted marketing

The Bureau should consider how it can use its UDAAP authority to prevent data brokers and their clients from discriminating against consumers in ways that are not covered by FCRA—although we reiterate that where FCRA applies, a FCRA violation is per se a UDAAP violation—to the extent that those entities fall within the Bureau's jurisdiction. We do not enumerate examples here as we believe FCRA generally should apply, especially if (as we argue) proxies for FCRA-covered data fall within the purview of FCRA. This is distinct from our recommendation about scoring above, in that it is conceivable that data brokers could utilize a discriminatory taxonomy that does not rely on a scoring methodology.[346]

---

[344] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, NPR (July 17, 2018), https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[345] *See, e.g.*, Merizwinski & Chester, *supra* note 313, at 873–74. *But see* NCLC FCR § 2.3.1.1 35 (citin *Tailford v. Experian Info. Sols., Inc.*, 2020 WL 2464797, at *6 (C.D. Cal. May 12, 2020)); Lubarsky, *supra* note 52.

[346] *See, e.g.*, Center for Democracy and Technology, EPIC, & Ranking Digital Rights, Comments on the FCC's Further Notice of Proposed Rulemaking regarding Empowering Broadband Consumers Through Transparency, CG Docket No. 22-2 (Feb. 16, 2023), https://epic.org/documents/in-the-matter-of-empowering-broadband-consumers-through-transparency-fnprm/ (citing FTC, A Look At What ISPs Know About You:

7. Regulate fraud scoring (to the extent not covered by FCRA)

If the Bureau does not treat fraud scoring and ID verification/authentication companies as CRAs, as we recommend above, it should more closely regulate entities that both perform these functions and are subject to the Bureau's authority under CFPA. As noted above, it is often impossible for a consumer to discern whether they were denied a product or service due to creditworthiness concerns or due to triggering a fraud detection system. This can be especially troubling for victims of ID theft, who are being denied services due to someone else's criminal conduct.

The Bureau should additionally closely examine the operations of fraud scoring and ID verification companies subject to its authority for fairness concerns[347] and require them to adequately secure the data used to make determinations about consumers.

8. Prohibit disclosure and purchasing of pre-conviction data

Regardless of whether the Bureau prohibits the use of pre-conviction data in credit reports under FCRA, as we recommend above, it should use its authority under CFPA to treat sharing pre-conviction data with third parties or purchasing pre-conviction data as presumptively harmful to consumers. Pre-conviction data does not reflect any determination about guilt or innocence, and the failure to update pre-conviction data with post-determination data can result in severe consequences for the individual.

Examining the Privacy Practices of Six Major Internet Service Providers 27 (2021), https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers) (describing some internet service providers' practices of placing consumers in segments based on protected classes or sensitive information, such as "viewership-gay," "pro-choice," "African American," "Jewish," "Asian Achievers," "Gospel and Grits," "Hispanic Harmony," "tough times," and "seeking medical care").

[347] *See* WPF Report at 53.

9. Create additional consumer protections for use of alternative credit data

A major challenge with alternative credit data is that it can exacerbate harms for vulnerable consumers.[348] To the limited extent that FCRA does not apply to this alternative data, the Bureau should use its UDAAP authority to extend the scoring protections to consumers we have described above: including disclosure by the company and the rights of access and correction by the consumer. The Bureau should also extend data security protections to alternative credit data.

10. Account for changes in technology

We applaud the Bureau's efforts to date but urge it to remain vigilant about how innovation may impact consumer interests. Technology consistently challenges our assumptions about privacy and data security.[349] Companies are likely able to identify individuals in various credit score brackets without accessing an actual score through the use of proxies, just as health risk scores can be derived from demographic data without using any specific patient data. Many companies have already reached the point at which they no longer need a CRA to perform analytics for them;[350] indeed, the FTC has flagged potential threats to competition resulting from the tremendous aggregations of data

[348] *See, e.g.*, NCLC, No Silver Bullet: Using Alternative Data for Financial Inclusion and Racial Justice 2 (2022), https://www.nclc.org/wp-content/uploads/2022/08/IB_Alt_Data_Is_No_Silver_Bullet-1.pdf (noting that rent reporting should be limited to only positive payment information; programs that report negative or "full file" information have the potential to hurt the most vulnerable).

[349] *See, e.g.*, 2011 FTC Staff Summary at 11 (rescinding guidance saying SSN-based coding was not unique identifier until decoded, to hold that identifier is unique if it could "otherwise reasonably be linked to the consumer"); EPIC Commercial Surveillance FTC Comments at 28–29; Population Reference Bureau & U.S. Census Bureau's 2020 Census Data Products & Dissemination Team, Why the Census Bureau Chose Differential Privacy, C2020BR-03 (2023), https://www2.census.gov/library/publications/decennial/2020/census-briefs/c2020br-03.pdf (addressing changes to Census in light of advances in re-identification methods); Press Release, NIST, NIST Announces First Four Quantum-Resistant Cryptographic Algorithms (July 5, 2022), https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (seeking to develop methods to resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today).

[350] *See* Hoofnagle, *supra* note 168, at 286; Hurley & Adebayo, *supra* note 313, at 187 ("For example, a lender that develops its own mechanisms for collection and data analytics will not trigger FCRA as long as it does not resell that information for further use in the credit, insurance, or employment context").

attempted by some firms.[351] We encourage the Bureau to explore the full extent of its authorities to help consumer protections keep pace with the breakneck pace of technological advancement.

ii. How the Bureau can prevent abusiveness in the data broker industry generally

The Bureau can exercise its abusiveness authority under the CFPA to enforce UDAAP violations by data brokers and their clients. As the Bureau outlines in its policy statement on abusiveness, there is no required showing of substantial injury to establish liability, as the conduct is itself the violation—conduct that Congress presumed to be harmful or distortionary to the proper functioning of the market.[352] This conduct includes (1) material interference with a consumer's ability to understand a term or condition of an offering; (2) taking unreasonable advantage of a consumer's lack of understanding of risks, costs, or conditions of an offering; (3) taking unreasonable advantage of a consumer's inability to protect their interests; and (4) taking unreasonable advantage of a consumer's reasonable reliance that the entity will act in the consumer's interests.[353] Our comments here focus on material interference, taking unreasonable advantage of a consumer's lack of understanding, and taking unreasonable advantage of a consumer's inability to protect their interests.

Material interference occurs when an act or practice intends to, has the natural consequence of, or actually results in impeding a consumer's ability to understand a term or condition.[354] The secrecy in which data brokers operate, the inescapability of data collection, and the current futility of "whack-a-mole" data deletion requests all fall within the scope of material interference with a

[351] *See, e.g.*, Chair Lina Khan et al., Joint Statement of Chair Khan, Commissioner Slaughter, Commissioner Wilson, and Commissioner Bedoya Regarding Amazon.com, Inc.'s Acquisition of 1Life Healthcare, Inc. (Feb. 27, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2210191amazononemedicalkhanslaughterwilsonbedoya.pdf.
[352] Abusiveness Policy Statement.
[353] *Id.*
[354] *Id.*

consumer's ability to understand the process necessary to **fully** opt out of data collection by data brokers.

Taking unreasonable advantage of a consumer's lack of understanding of the material risks, costs, or conditions of a product or service occurs even when the lack of understanding did not arise as a result of the covered entity's conduct; it occurs when this gap in understanding is exploitative.[355] Downstream misuses could serve as an example of this—for example, when custodians of utility data sell it to immigration authorities.

Taking unreasonable advantage of a consumer's inability to protect their interests can occur when the consumer has no meaningful choice in a particular provider, including credit reporting companies.[356] The "interests" consumers are entitled to protect include but not limited to property, privacy, and reputational interests; it applies to the use of a service even if the consumer did not select the service, and it includes situations in which it is impractical for consumers to protect their interests (e.g., when steps necessary to protect interests are unknown or are especially onerous).[357] Data access, correction, and deletion processes that are unknown or onerous to consumers fall within this scope, if only insofar as they frustrate the consumer's attempt to protect their autonomy interests in how their data is used.[358] In general, tactics that cultivate "a feeling of resignation"[359] fall within this scope.

A consumer often does not get to choose which dossier about themselves is presented on their behalf as a prospective customer (in both a FCRA context and in the context of some types of targeted marketing that may fall outside the scope of FCRA), and may not even be aware that a

[355] *Id.*
[356] *Id.*
[357] *Id.*
[358] *See, e.g.*, Hoofnagle, *supra* note 168, at 173 (explaining that data collection is too prolific for consumers to avoid it and that consumers are not in a position to hold data collectors accountable for how downstream brokers use their data).
[359] Knowledge at Wharton Staff, *supra* note 34.

dossier was used at all. Moreover, that dossier may put them in a category or categories they do not identify with (even if that categorization does not constitute a traditional reputational harm) or put them in a category with which they do identify but which can result in harm if disclosed (e.g., the Catholic priest harmed by disclosure of data collected by Grindr). Additionally, that dossier may result in a loss of opportunity or discrimination (either from certain offers being displayed to the consumer but not to other consumers, or from being excluded from seeing certain ads), which falls within the scope of abusiveness. This would likely include shadow profiles discussed above.

Sharing data about a consumer that can be reidentified also falls within this scope, as the consumer is not able to protect their privacy interests after the purportedly deidentified data has been shared. This could also constitute deception if the covered entity represented to the consumer that the data was deidentified, and unfairness if it resulted in substantial injury. But even without any representation by the company or injury suffered by the consumer, it constitutes an abusive act or practice. Cross-device tracking and shadow profiles could fall under this umbrella as well.

We encourage the Bureau to explore the contours of its abusiveness authority as it relates to data brokers and the systems in which they operate.

iii. The Bureau can use its larger market participant supervisory authority to regulate the data broker industry

Since September 30, 2012, any nonbank entity with more than $7 million in annual receipts resulting from consumer reporting activities[360] is considered a larger participant in the consumer reporting market and is subject to the Bureau's supervisory authority under the CFPA.[361] While this would not impact many smaller data brokers, it would apply to larger market participants such as

[360] This definition is not co-extensive with FCRA. NCLC FCR § 2.3.1.1 32 (citing 77 Fed. Reg. 42874, 42885 (July 20, 2012), https://www.federalregister.gov/d/2012-17603/p-143 (CFPB noting difference in definitions)).
[361] Defining Larger Participants of the Consumer Reporting Market, 77 Fed. Reg. 42873, 42874, 43875 (July 20, 2012), https://www.federalregister.gov/d/2012-17603/p-11.

LexisNexis.[362] The Bureau's supervisory authority empowers it to assess compliance with federal consumer financial laws and regularly entails releasing reports and guidance to inform and advise regulated entities. Notably, this authority can also provide additional transparency and accountability regarding covered entities using consumer scoring systems and non-score-based targeted marketing methodologies, as the Bureau can examine and publish reports on how those systems operate.[363] It is also significant that the Bureau explicitly noted that it will exercise this authority over entities beyond those FCRA defines as CRAs and that it will seek to detect and assess risks to consumers and markets for consumer financial products or services.[364]

d. Other Bureau authorities

Although we do not detail them here, we note that the Bureau has other authorities which may be relevant to its regulation of data brokers, including the Equal Credit Opportunity Act, the Gramm-Leach-Bliley Act, and the Truth in Lending Act.

VI. Conclusion

We applaud the CFPB's ongoing efforts to understand the growing impacts of data brokers on consumer privacy, data security, and consumer access to financial, credit, employment, and other opportunities. The CFPB can and should use its authority under the FCRA, CFPA, and related laws to regulate data brokers and protect consumers from harmful data collection and use practices. Doing so will not undermine competition or jeopardize consumer rights.

We appreciate this opportunity to comment and are willing to engage with the agency further on any of the issues raised within our comment, including but not limited to data minimization, fraud detection and ID verification, data anonymization and de-anonymization, data security, and the

[362] *See, e.g.*, OSF Data Brokers Report at 170 (estimated revenue from LexisNexis Risk Solutions alone was $1.58BB in 2014).
[363] *See* Mierzwinski & Chester, *supra* note 313, at 878–79.
[364] 77 Fed. Reg. at 42885.

consumer impacts of unregulated automated decision-making. These issues not only relate closely to how data brokers impact consumer data rights and consumer access to financial and other opportunities, but may also serve as a foundation for clarifying data brokers' obligations under the FCRA, CFPA, and similar laws.

Respectfully submitted,

/s/ *John Davisson*
John Davisson
Director of Litigation

/s/ *Ben Winters*
Ben Winters
Senior Counsel

/s/ *Christopher Frascella*
Christopher Frascella
Law Fellow

/s/ *Grant Fergusson*
Grant Fergusson
Equal Justice Works Fellow

/s/ *Suzanne Bernstein*
Suzanne Bernstein
Law Fellow