CENTER FOR DEMOCRACY & TECHNOLOGY

March 6, 2023

To: National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Request for Comments on Privacy, Equity, and Civil Rights, NTIA-2023-0001

Table of Contents

CENTER FOR DEMOCRACY & TECHNOLOGY

Introduction

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comments (RFC) addressing issues at the intersection of privacy, equity, and civil rights. CDT is a nonprofit 501(c)(3) organization dedicated to advancing privacy, consumer, and civil rights for all in the digital age. CDT was glad to participate in the NTIA's listening session on the privacy and civil rights landscape in December 2021,[1] and we are heartened by the NTIA's continued commitment to guiding the federal government's understanding of and response to technology-related harms to marginalized communities.

Our comments begin by describing a variety of data practices that disproportionately harm marginalized people, and explaining how existing privacy and civil rights laws address these harms or fall short of doing so effectively. Next, our comments explain how stakeholders should approach the implications of these harmful practices. Then, we propose guiding principles and actions to help the federal government to respond to these concerns.

I. Examples of harms to certain marginalized communities

(Questions 1c, 1d, 1e, 1f, 1g, 2, 2a, 2b, 2c, 3, 3a, 3b, 3c, 3d, 4, 4a, 4b, 4c, and 4d)

Several prevalent data practices produce systemic, widespread patterns of harms – targeted to individual people or certain groups, or encountered by society as a whole. The RFC reflects the NTIA's deep engagement with advocates and researchers for over a year to understand how common data practices harm different groups. The RFC rightfully recognizes that the impacts of these practices can vary for numerous marginalized identities and groups, including those not traditionally protected under civil rights laws. To illustrate these impacts, below we discuss five examples of categories of practices that disproportionately affect marginalized communities:

- The collection and use of sensitive information;
- Data brokers' sharing or sale of data for purposes to which the person from whom the data is gathered does not consent;
- The collection and use of consumer data to target advertising;

[1] Center for Democracy & Technology, *Protecting Disabled People's Privacy is a Civil Rights Issue: Lydia X. Z. Brown's Remarks Before the NTIA's Listening Session on Civil Rights, Privacy, and Data* (Dec., 14, 2021), https://cdt.org/insights/protecting-disabled-peoples-privacy-is-a-civil-rights-issue-lydia-x-z-browns-remarks-before-the-ntias-listening-session-on-civil-rights-privacy-and-data/.

- Discriminatory data- or algorithm-driven decisions that limit access to housing, credit, and employment;
- Data collection through dark patterns that curtail consumer choice.

A. The heightened risks of collecting and repurposing sensitive data

(Questions 1c, 2, 2a, 2b, 2c, 3, 3a, 3b, and 3c)

Many online companies collect, use, share, and otherwise process sensitive data. Sensitive data includes, among other categories, health and financial data, content of communications, identification numbers, biometric information, location, and demographic information.[2] It can reveal insights about people like their financial situation, the parties to and substance of their communications, disability status, health, movements and travels, and sexual activity. Its inappropriate use can lead to financial, reputational, physical, and emotional harm.[3] Below, we discuss harms resulting from the overcollection and use of four examples of specific types of sensitive data – namely disability-related data, health data, location data, and financial data – and the limitations of existing privacy and civil rights laws in addressing them.

i. Disability-related data

(Questions 2, 2a, and 2b)

CDT's work has explored the wide-ranging impacts of commercial data practices on disabled people that cause or further perpetuate existing discrimination and prejudice.[4] Disabled people have a long history of experiencing online discrimination. People with physical and mental

---

[2] *See e.g.* § 2(28)(a) of the "American Data Privacy and Protection Act" (H.R. 8152).

[3] Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 Boston U. L. Rev. 793, 831-45 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222. Simply knowing that you are being surveilled can have real consequences for peoples' mental health. *See* Saumya Kalia, *What is a Constant Lack of Digital Privacy Doing to Our Mental Health?*, The Swaddle (Jan. 26, 2022), https://theswaddle.com/what-is-a-constant-lack-of-digital-privacy-doing-to-our-mental-health/.

[4] *See* Lydia X. Z. Brown, Ridhi Shetty, Matthew U. Scherer, & Andrew Crawford, Center for Democracy & Technology, *Ableism And Disability Discrimination in New Surveillance Technologies* (2022), https://cdt.org/insights/ableism-and-disability-discrimination-in-new-surveillance-technologies-how-new-surveillance-technologies-in-education-policing-health-care-and-the-workplace-disproportionately-harm-disabled-people/ [hereinafter Brown, *Surveillance Technologies*]; Center for Democracy & Technology, *Comments to Office of Science and Technology Policy Regarding Public and Private Sector Uses of Biometric Technologies*, Jan. 15, 2022, https://cdt.org/wp-content/uploads/2022/01/CDT-Comments-for-OSTP-RFI-on-biometrics-2021-21975.pdf (discussing the impact of biometric technologies on disabled people); Center for Democracy & Technology, *Comments to United Nations Special Rapporteur on the Rights of Persons with Disabilities Regarding the Impacts of Artificial Intelligence on People with Disabilities*, Nov. 3, 2021, https://cdt.org/wp-content/uploads/2022/01/CDT-Comments-for-OSTP-RFI-on-biometrics-2021-21975.pdf.

disabilities face substantially higher likelihood of potentially invasive personal data collection for a range of reasons, including discrimination that creates further records such as through evictions or arrests,[5] and through interactions with governmental entities because of greater reliance on public benefits and social services.[6]

Some disabled people are also more likely to need or want to use health-related apps and platforms, but these apps and platforms can exploit the sensitive disability-related data people are required to share to use these services. For example, Mozilla researchers found that mental health (as well as prayer apps) fare worse than any other product category they examined with regards to protecting people's privacy and security.[7] The apps Mozilla reviewed routinely collected, retained, and shared sensitive data about users' conditions like depression, anxiety, suicidality, victimization by domestic violence, disordered eating, and post-traumatic stress disorder.[8] This includes heavily promoted therapy apps like BetterHelp and Talkspace that share user data with Facebook – users' presence on these apps itself is a data point that can be exploited for marketing.[9] Pride Counseling, an app specifically designed for the LGBTQ+ community, suffers from similar concerns as its parent company, BetterHelp, and it does not clarify whether users have to opt in or opt out to avoid their data being repurposed for marketing.[10]

Mozilla further found that certain apps also allow weak passwords, target users with personalized ads, and feature vague and poorly written privacy policies that are too ambiguous regarding the kinds of data they accumulate and how they use it. For instance, the Better App Company's suicide prevention app offers a privacy policy that appears incomplete and is certainly unclear about its data collection and sharing and how its data use supports people experiencing suicidality or a mental health crisis, both of which are disability-related experiences.[11] NOCD, which aims to help people manage obsessive compulsive disorder, shares

[5] *See* Sec. I(D)(i).
[6] *See* Sec. I(D)(iv)-(v).
[7] Mozilla, *Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security* (May 2, 2022), https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/.
[8] *Id.*
[9] Thomas Germain, *Mental Health Apps Aren't All as Private as You May Think*, Consumer Reports (Mar. 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/.
[10] Pride Counseling, *Privacy Policy* (last updated Sept. 21, 2022), https://www.pridecounseling.com/privacy/ (stating that data will be disclosed to advertising partners if users opt in to targeting cookies, but also that users should follow certain steps to opt out of cookies).
[11] The Better App Company, *Privacy* (last updated Sept. 14, 2018), https://www.thebetterappcompany.com/privacy.

personal non-health user data (of a user base defined by a disability diagnosis) with data analytics providers like Google and Meta for targeted advertising.[12]

Some companies collect people's mental health data from social media posts and then take well-intentioned, but potentially harmful or unhelpful, action related to that information. For instance, social media platforms like Facebook reportedly have algorithms that purport to detect suicide risk, and they may flag content and either transmit this information to law enforcement that is ill-equipped to engage disabled people in need of support, or refer people to resources that they may not find helpful either to address an immediate crisis or seek long-term support.[13]

Many Internet of Things (IoT) devices and internet-connected assistive technologies can store excessive amounts of data – the inherent privacy risk is a tradeoff that people with certain disabilities may be obligated to accept because they rely on the support these technologies can offer to independently perform certain tasks that might otherwise require another person's assistance.[14] These technologies can, for instance, help people with physical disabilities manage their home lighting, temperature, or security systems.[15] However, the data collected through these technologies is subject to third-party data-sharing and cloud storage, which could make users vulnerable to data breaches.[16]

Some of this data includes biometric data processed for security purposes, while other data can convey information about a person's daily habits and activities to third parties. For instance, data analytics company Verisk gathers behavioral data from smart home devices to inform

---

[12] NOCD, *Privacy Policy* (last updated Aug. 3, 2022), https://www.treatmyocd.com/privacy-policy.
[13] Karen L. Celedonia, Marcelo Corrales Compagnucci, Timo Minssen, & Michael Lowery Wilson, *Legal, Ethical and Wider Implications of Suicide Risk Detection Systems in Social Media Platforms*, J. L. Biosci. (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8284882/; Benjamin Goggin, *Inside Facebook's Suicide Algorithm: Here's How the Company Uses Artificial Intelligence to Predict Your Mental State From Your Posts*, Bus. Insider (Jan. 6, 2019, 11:19 AM), https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12.
[14] *See* Henry Claypool, Claire Carey, Alexander C. Hart, & Linnea Lassiter, American Association of People with Disabilities and Center for Democracy & Technology, *Centering Disability in Technology Policy: Issue Landscape and Potential Opportunities for Action* 41 (2021), https://cdt.org/wp-content/uploads/2021/12/centering-disability-120821-1326-final.pdf.
[15] *Id.*
[16] Lauren Smith, Carson Martinez, Chanda Marlowe, & Henry Claypool, Future of Privacy Forum, *The Internet of Things (Iot) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions* 10-14 (2019), https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.

insurers' risk evaluations for life, auto, and property insurance products.[17] This practice increases the risk of harm to disabled people who rely on internet-connected assistive technologies because insurers can repurpose data collected from these devices to terminate coverage or increase premiums for a group of people more likely to include disabled users.[18] The risk is even greater in light of the fact that smart home devices are already known to be susceptible to security breaches – for example, hackers have been able to take control of Google Nest and Amazon Ring devices to harass people in their homes.[19]

ii. Health data

(Questions 2, 2c, 3, and 3a)

Health data (both disability-related and unrelated to disability) is particularly private and has historically been provided extra protections like those found in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA and its associated Privacy Rule place limitations on the disclosure and sharing of protected health information.[20] However, as the RFC recognizes, HIPAA does not address all health data. Instead, HIPAA's privacy protections apply to health data only when it is in the possession of "covered entities" – doctors, insurance companies, and those who support them. HIPAA does not apply when health data is held by a non-covered entity – like health and wellness apps, wearable fitness trackers, websites, and data brokers. The ever-increasing use and popularity of these health-related apps, devices, online services, and IoT has resulted in extraordinary amounts of information reflecting mental and physical health being collected, retained, shared, and used by entities that are not bound by

[17] Verisk, *The Verisk Data Exchange: Personal and Commercial Property IoT*, https://www.verisk.com/insurance/capabilities/telematics/property-iot/; Sandra Maples, *How Smart Devices are Providing the Data Claims Professionals Need*, Verisk (Oct. 3, 2017), https://www.verisk.com/insurance/visualize/how-smart-devices-are-providing-the-data-claims-professionals-need/.

[18] Tenzin Wangmo, Mirjam Lipps, Reto W. Kressig, & Marcelo Ienca, *Ethical Concerns With the Use of Intelligent Assistive Technology*, 20 BMC Med. Ethics 8, https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-019-0437-z.

[19] Hayley Peterson, *Wisconsin Couple Describe the Chilling Moment That a Hacker Cranked Up Their Heat and Started Talking to Them Through a Google Nest Camera in Their Kitchen,* Business Insider (Sept. 25, 2019, 4:12 PM), https://www.businessinsider.com/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple-2019-9; Kari Paul, *Dozens Sue Amazon's Ring After Camera Hack Leads to Threats and Racial Slurs*, The Guardian (Dec. 23, 2020, 4:40 PM), https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats.

[20] Department of Health & Human Services, *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

HIPAA obligations. Regulations finalized in spring 2020 further shrunk the categories of HIPAA-protected data.[21]

One example that illustrates this gap is Flo, a reproductive health app that collected sensitive health data (like dates of menstrual cycles, when pregnancies started and ended, menstrual and pregnancy-related symptoms, weight, and temperature) from its millions of users and shared that data with outside analytics providers.[22] Though Flo told people that their sensitive health data would be shared and used in limited ways, Flo was actually sharing people's data with a number of third parties for purposes unrelated to the core service provided by the app. The FTC ordered Flo to obtain affirmative express consent from people before sharing sensitive health data with third parties.[23] More recently, Flo began offering an "anonymous mode" that allows users to prevent the sharing of any unique user identifiers.[24] Similarly, GoodRX, an app used to find discounts on prescriptions, was found to be sharing users' contact information with Facebook, Google, and other platforms to enable targeted advertising of certain medications to those users.[25]

Health-related data collected, shared, and used by consumer-facing tech can be extremely personal and sensitive, and inappropriate use or sharing of such data can lead to a variety of harms. For example, data about conditions that are especially sensitive because of accompanying, unwarranted prejudice can lead to social stigmatization, discrimination or even threats of violence. An analysis of the 2017 National Crime Victimization Survey found that LGBTQ+ people are nearly four times more likely than non-LGBTQ+ people to experience violent

[21] 85 Fed. Reg. 25642 (May 1, 2020) and 85 Fed. Reg. 25510 (May 1, 2020). For a comprehensive review of the current legal landscape governing health data and the gaps in protection for the same, *see* Robert Belfort, William S. Bernstein, Alex Dworkowitz, Brenda Pawlak, and Po Yi, Manatt, *A Shared Responsibility: Protecting Health Data Privacy in an Increasingly Connected World* (2020), https://www.manatt.com/Manatt/media/Media/PDF/White%20Papers/Healthcare-Whitepaper-RWJF-Protecting-Consumer-Health-Data-Privacy-in-an-Increasingly-Connected-World_e.pdf.
[22] Complaint, In the Matter of Flo Health, Inc., File No. 1923133 (2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.
[23] *Id. See also* Decision and Order, In the Matter of Flo Health, Inc, File No. 1923133 (2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf.
[24] Flo, *Flo Anonymous Mode Overview* (2022), https://flo.health/flo-health-inc/news/anonymous-mode-whitepaper.
[25] Natasha Singer, *GoodRX Leaked User Health Data to Facebook and Google, FTC Says*, N.Y. Times (Feb. 1, 2023), https://www.nytimes.com/2023/02/01/business/goodrx-user-data-facebook-google.html.

victimization by people they know and by strangers.[26] Because parts of the LGBTQ+ community experience disproportionately higher rates of HIV, exposing that a person is HIV-positive potentially puts them at heightened risk of violence.[27]

Just such a risk arose when an app used by members of the LGBTQ+ community, the dating app Grindr, shared user data in an unfair and harmful manner.[28] Grindr "provided users' HIV status and GPS location data, along with other profile details including email addresses, to two companies hired to test the app's technical performance."[29] News accounts noted that "[b]ecause Grindr users would have reasonably expected the app to be vigilant in guarding such information, its failure to do so is not only a breach of their privacy but an actual harm."[30]

Potential harms from collection and sharing of health information can also extend to risk of investigation, litigation, and prosecution. The recent overturning of *Roe v. Wade* in *Dobbs v. Jackson Women's Health Organization*,[31] and subsequent criminalization of abortion in some states, has created new cause for concern about reproductive health data. Such data, whether collected directly from an online company or from a data broker, could be used to enforce those laws if it reveals that a person obtained, or attempted to obtain, an abortion or aided another in doing so. For example, anti-choice groups have used data linked to people's advertising IDs on their smartphones to target patients and send pro-life advertisements "directly to a woman's phone while she is in a clinic waiting room."[32] The same technology "also has the capability to hand the names and addresses of women seeking abortion care, and those who provide it, over to anti-choice groups."[33] In the wake of *Dobbs,* that data could be used in some states by law enforcement to launch criminal investigations and prosecutions, as well as civil suits by "bounty

---

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

[27] Human Rights Campaign, *How HIV Impacts LGBTQ People* (Feb. 2017), https://www.hrc.org/resources/hrc-issue-brief-hiv-aids-and-the-lgbt-community.

[28] Alison Bateman-House, *Why Grindr's Privacy Breach Matters to Everyone*, Forbes (Apr. 10, 2018, 10:09 AM), https://www.forbes.com/sites/alisonbatemanhouse/2018/04/10/why-grindrs-privacy-breach-matters-to-everyone/?sh=2a09490567f4.

[29] *Id.*

[30] *Id.*

[31] 597 U.S. ___ (2022).

[32] Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, Rewire News Group (May 25, 2016, 6:52 PM), https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/.

[33] *Id.*

hunters" against those seeking abortions.[34] That risk remains even when people go out of their way to attempt to keep their reproductive health data private since it is difficult to avoid collection of all data that may be revealing about reproductive health care choices.[35]

Data broker Kochava allegedly sold location information about millions of mobile devices that could reveal people's visits to sensitive locations like reproductive healthcare clinics and addiction treatment facilities.[36] Kochava is not the only data broker putting people's health data at risk: SafeGraph and PlacerAI are among others collecting and sharing data about the locations and durations of people's visits to reproductive health clinics, which could cause significant monetary harm or even imprisonment.[37] This risk is particularly troubling as new, obscure sources of reproductive health data emerge: one new wellness start-up called 28 uses basic menstrual cycle data to make lifestyle recommendations; while it claims to only "voluntarily collect" data and to keep it "strictly confidential," its privacy policy indicates more expansive collection of data that will be disclosed to third parties.[38]

People can be harmed when health data is used as part of a profile that results in them being denied, or not even offered, economic opportunities. A *New York Times* investigative piece from May 2021 examined the data and privacy practices of 250 iPhone apps and revealed that of the twenty health apps they reviewed, "13 apps shared with an average of three third-party trackers."[39] The *Times* piece goes on to note that, while it is difficult to track exactly how some of the third parties that receive data about users' health use that information, they do know that some data is used by tools that can "generate a health-risk prediction score that is then provided to life insurance companies to assess whether people may be interested in their

---

[34] Albert Fox Cahn & Eleni Manis, *Surveillance Technology Oversight Project, Pregnancy Panopticon: Abortion Surveillance After Roe* (2022), https://www.stopspying.org/pregnancy-panopticon.
[35] Anya E.R. Prince, *I Tried to Keep My Pregnancy Secret*, The Atlantic (Oct. 10, 2022), https://www.theatlantic.com/ideas/archive/2022/10/can-you-hide-your-pregnancy-era-big-data/671692.
[36] Complaint, Federal Trade Commission v. Kochava, No. 2:22-cv-377 (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
[37] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, Vice (May 3, 2022, 12:46 PM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood; Joseph Cox, *Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live*, Vice (May 5, 2022, 8:24 PM), https://www.vice.com/en/article/g5qaq3/location-data-firm-heat-maps-planned-parenthood-abortion-clinicsplacer-ai.
[38] Natasha Lomas, *Cycle-Focused Femtech Startup, 28, Grabs Backing From Thiel Capital*, TechCrunch (Aug. 23, 2022, 9:10 AM), https://techcrunch.com/2022/08/23/28-seed-thiel-capital/; 28, *Privacy Policy* (last modified Sept. 7, 2022), https://28.co/privacy.
[39] Thorin Klosowski, *We Checked 250 iPhone Apps – This is How They're Tracking You*, N.Y. Times: Wirecutter (May 6, 2021), https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/.

product."[40] Researchers at the University of Pennsylvania have also documented how most health-related websites track people who visit each site.[41] The researchers note that this health data can not only be used to target ads but may also include "much more damaging privacy loss and the domino effect that could have on credit scores, insurance coverage, and many as-yet-undiscovered facets of someone's life."[42] Likewise, sharing consumer health data with an employer can have real-life impacts on access to a job.[43]

As described in CDT's report, *Placing Equity at the Center of Health Care & Technology*, when data from consumer-facing tech is being used for health purposes like diagnosis or access to benefits, inaccurate, unrepresentative, or incomplete data can result in negative health outcomes, or in lost or denied services and benefits, especially for people from underrepresented and overlooked communities.[44] For instance, *Wired* reported that predictive health technologies frequently rely upon skewed, unrepresentative data sets that "are the norm in health AI research, due to historical and ongoing health inequalities."[45]

Finally, certain data practices limit individual autonomy and can cause collateral harms in other areas of life. For example, people used the Crisis Text Line, a nonprofit mental health hotline, to seek help for problems such as suicidal thoughts, anxiety, and emotional abuse. When using the service, people disclosed highly personal and sensitive information. While users expected their data would be kept private, news reports exposed how the Crisis Text Line shared people's personal and sensitive data with a for-profit spinoff.[46] The company ended this data-sharing relationship after reports detailing its troubling data practices emerged.[47]

---

[40] *Id.*
[41] Michele W. Berger, *What Can Browser History Inadvertently Reveal About a Person's Health?*, University of Pennsylvania: Penn Today (Apr. 29, 2022), https://penntoday.upenn.edu/news/what-browser-history-inadvertently-reveals-Penn-CMU-digital-health-privacy-initiative.
[42] *Id.*
[43] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?*, Wash. Post (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.
[44] Andrew Crawford, Center for Democracy & Technology, *Placing Equity at the Center of Health Care & Technology* 13 (2022), https://cdt.org/wp-content/uploads/2022/03/2022-03-22-CDT-Placing-Equity-at-the-Center-of-Health-Care-Technology-final.pdf [hereinafter Crawford, *Placing Equity*].
[45] Tom Simonite, *When It Comes to Health Care, AI Has a Long Way to Go*, Wired (Jan. 16, 2022, 7:00 AM), https://www.wired.com/story/health-care-ai-long-way-to-go/.
[46] John Hendel, *Crisis Text Line Ends Data-Sharing Relationship With For-Profit Spinoff*, Politico (Jan. 31. 2022, 8:37 PM), https://www.politico.com/news/2022/01/31/crisis-text-line-ends-data-sharing-00004001.
[47] *Id.*

The risk of these and other harms is unfortunately high. Many health apps are failing at protecting privacy. Last year, the International Digital Accountability Council (IDAC) released a report that assessed the consumer protection risks of 152 digital health apps that utilize the most sensitive personal information, and classified these apps into three categories: femtech, mental health, and fitness and weight loss.[48] IDAC's report details that "some widely-used apps fail to meet even basic platform requirements because they send unencrypted user data, have inadequate or missing privacy policies, or collect granular information about user location without adequate explanation."[49]

The findings did not stop there. IDAC continued that "the majority of apps investigated have questionable practices and disclosures around third-party data sharing, illustrating a clear mismatch between current legal protections and the widespread collection and sharing of sensitive health information."[50] For example, in some instances IDAC investigators "observed transmission of users' advertising identifiers to at least one third-party endpoint that was not disclosed in the app's privacy policy."[51] Even when apps made some disclosures to users, some failed to state all the third-party services that IDAC observed.[52] IDAC noted that even in instances when "apps carefully follow existing rules, most users have little visibility into how their information is collected or shared."[53]

iii. Location data

(Questions 1e, 2, 2a, 3b, and 3c)

A broad variety of apps and tools often collect and then share users' location data with third parties for no purpose, or for purposes unrelated to the actual services these apps or tools provide. The *New York Times'* examination of 250 apps, discussed above, found that numerous shopping, news, and dating apps gather and share location data.[54] Of the twenty weather apps examined, for example, fourteen used location information to track devices. Similar concerns

[48] The report examined 152 Android health apps that were available in the Google Play Store as of November 10, 2021, selected using keyword search results. Holden Williams, Ginny Kozemczak, and Dan Kinney, Int'l Digital Accountability Council, *Digital Health is Public Health: Consumers' Privacy & Security in the Mobile Health App Ecosystem* (2021), https://secureservercdn.net/198.71.190.114/99x.577.myftpupload.com/wp-content/uploads/2022/01/Digital-Health-is-Public-Health-People-Privacy-and-Security-in-the-Mobile-Health-App-Ecosystem.pdf.
[49] *Id*. at 1.
[50] *Id.* at 2.
[51] *Id.* at 12.
[52] *Id.*
[53] *Id.* at 2.
[54] Klosowski, *supra* note 39.

extend to apps that do not need location data to function and only collect it for purposes such as advertising. For example, Goldenshores Technologies, the developer of the Brightest Flashlight app, faced an enforcement action for its location data collection and sharing practices.[55] Mobile game apps like "Angry Birds" were also reported to collect location and other data and transmit it to government entities.[56] And many of the data brokers collecting location data for reproductive purposes came from the software development kits of apps that were collecting location for no, or other, purposes.[57]

Location data can reveal people's private activities, such as their visits to health clinics or places of worship.[58] For instance, Kochava collected and then sold people's precise geolocation data in a format that allowed entities to track people's "movements to and from sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at risk populations, and substance use recovery."[59] Additionally, late last year, *The Markup* published a story that detailed how Life360, a popular family safety app, was selling location data about its users to data brokers.[60] After the story was published, "Life360 announced that it will stop sales of precise location data to the dozen or so data brokers it had been working with, and will now sell only precise location data to Arity and 'aggregated' location data to PlacerAI."[61] Some prayer apps also share users' location data,

---

[55] Federal Trade Commission, Press Release, Android Flashlisht App Developer Settles FTC Charges it Deceived People (Dec. 5, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived-people.

[56] James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, The Guardian (Jan. 28, 2014, 2:51 AM), https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data.

[57] Joseph Cox, *Data Broker is Selling Location Data of People Who Visit Abortion Clinics*, Vice Motherboard (May 3, 2022, 12:46 PM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

[58] Andrew J. Blumberg & Peter Eckersley, Electronic Frontier Foundation, *On Locational Privacy, and How to Avoid Losing it Forever* (2009), https://www.eff.org/wp/locational-privacy; Samantha Lai & Brooke Tanner, Examining the Intersection of Data Privacy and Civil Rights, Brookings (July 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights.

[59] Complaint, Federal Trade Commission v. Kochava, *supra* note 36.

[60] Jon Keegan & Alfred Ng, *The Popular Family Safety App Life 360 is Selling Precise Location Data on Its Tens of Millions of Users*, The Markup (Dec. 6, 2021, 8:00 AM), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

[61] *Id.*

which can be obtained by the government.[62] Indeed, the Council on American-Islamic Relations filed a complaint earlier this year describing how the sale of location data to government agencies constitutes a deceptive practice for users in general and an unfair practice particularly for historically hyper-surveilled communities.[63]

Identified location data is not the only type of location data that poses risks: the *New York Times* was able to review anonymized location data and conclude that "[i]n most cases, ascertaining a home location and an office location was enough to identify a person."[64] As a result, companies can use location data to infer people's activities and make decisions accordingly, such as increasing insurance rates based on where people are traveling, or scrutinizing prospective rental applicants' activities.[65]

When used in unwanted, unanticipated, or unknown ways, even anonymized data can allow inferences specific to marginalized people. Last year, a priest resigned after a Catholic media site obtained location data from the dating app Grindr to reveal his visits to gay bars.[66] A user's location data indicating that they have gone to a venue catering to LGBTQ+ communities was also shared with the app's advertising partners to target LGBTQ+-related advertisements; others accessing the user's device might then see such ads, which could out the user to those close to them.[67]

iv. Financial data

(Questions 2, 3, and 3a)

[62] Mozilla, supra note 7; Joseph Cox, How the U.S. Military Buys Location Data From Ordinary Apps, Vice (Nov. 16, 2020, 10:35 AM), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
[63] Complaint, In the Matter of Request for Investigation of Alleged Violations of Section 5 of the FTC Act by Multiple Actors in the Location Data Industry (2022), https://www.cair.com/wp-content/uploads/2022/04/FTCcomplaint.pdf.
[64] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.
[65] Keegan, *supra* note 60; Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone,* Vice Motherboard (Jan. 18, 2019, 12:08 PM).
[66] Michelle Boorstein, Marisa Iati, and Annys Shin, *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, Wash. Post (July 21, 2021, 8:21 AM), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.
[67] Sarah Syed, Natalia Drozdiak, & Nate Lanxon, *Grindr Shares Location, Sexual Orientation Data, Study Shows*, The Detroit News (Jan. 14, 2020, 10:22 AM), https://www.detroitnews.com/story/business/2020/01/14/grindr-shares-location-sexual-orientation-data-study-shows/40997573/; Chris Wood, Katelyn Ringrose, Carlos Gutierrez, Amie Stepanovich, & Connor Colson, LGBT Tech and Future of Privacy Forum, *The Role of Data Protection in Safeguarding Sexual Orientation* 9, 13 (2022), https://www.lgbttech.org/_files/ugd/1b643a_21883c316e1547c99c6a1d997688f975.pdf.

People have more options than ever to make payments and transfer funds online, which means that financial data is proliferating online and can put people at risk. This information includes names, addresses and other contact information, credit card numbers, bank account information, dates of birth, Social Security numbers, banking activity, transaction history, and purchase activity, which can make people vulnerable to data misuse when accessed by third parties.[68] Much of this data is stored not only by financial institutions, but also by online retailers and large and start-up financial technology (or fintech) platforms.[69] One risk arising from the overcollection and sharing of financial data is that of identity theft, fraud, and other financial crimes. For example, the more entities that possess and store this information, the greater the risk of a breach or other unauthorized access by bad actors.

Misuse of financial data also gives rise to other risks. Technology companies that have historically used consumer data for a whole host of non-financial purposes, from communication and social networking to navigation to media streaming, have introduced payment processing services. This adds financial data to the wealth of data that companies with burgeoning online advertising businesses can wield to profile people's behavior for potential profit. For instance, Meta and Amazon use and share people's purchase activity, along with other data such as location and device identifiers, to tailor advertisements, measure how well products are meeting the companies' goals, and inform new products.[70] This also makes it harder for people to discern the purposes for which they can expect the companies to use financial data.

Companies that have mainly used people's financial data to provide online payment processing services now use and share data for marketing as well. PayPal shares people's contact information, bank account and purchase data, and IP addresses with a wide network of third parties for more expected purposes like payment processing and fraud detection, but also for

---

[68] Center for Democracy & Technology, *Comments Regarding CFPB Inquiry Into Big Tech Payment Platforms*, at 3, (Dec. 20, 2021), https://cdt.org/wp-content/uploads/2021/12/CDT-Comments-to-CFPB-on-Big-Tech-Payment-Systems-Docket-No-CFPB-2021-0017.pdf.

[69] Stan Adams & John Morris, Jr., Center for Democracy & Technology, *Open Banking: Building Trust* (2021), https://cdt.org/wp-content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf.

[70] Meta, *Privacy Policy* (effective July 26, 2022), https://www.facebook.com/privacy/policy/?section_id=2-HowDoWeUse; Amazon, *Amazon.com Privacy Notice* (last updated Jun. 29, 2022), https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ.

less anticipated purposes like personalization and marketing.[71] In 2019, Mozilla researchers demonstrated the ease with which Venmo users' transaction data could be used to gain insights about users' social connections and financial and non-financial personal activity, which in turn facilitates stalking and fraudulent use of identifiable data.[72]

Existing laws relevant to protecting financial data only go so far. The Gramm-Leach-Bliley Act only applies to financial institutions, which have not been clearly defined to include the technology companies and data aggregators whose access to and control over financial data has grown.[73] The Fair Credit Reporting Act (FCRA) imposes obligations on entities who evaluate and assemble consumer data to furnish it to other entities for enumerated permissible purposes.[74] Marketing is not among these permissible purposes, but companies that use consumer data for marketing argue that they are not consumer reporting agencies and thus are not liable under the FCRA.

B. Data brokers make sharing of generally "non-sensitive" data riskier

(Questions 1c, 1e, 2, 2a, 2b, 2c, 3, 3a, 3b, 3d)

As described above, sensitive health, location, and financial data are major targets for data brokers, which are companies that knowingly collect data about people from sources other than the consumer themselves and sell the data to third parties.[75] However, data brokers traffic in all kinds of data, as we learned from the 2013 and 2014 reports from the Senate Committee on Commerce, Science, and Transportation and the FTC (respectively) analyzing the privacy risks

[71] PayPal, *List of Third Parties (Other Than PayPal Customers) With Whom Personal Information May be Shared* (effective Oct. 1, 2022), https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list.
[72] Letter from Electronic Frontier Foundation and Mozilla to PayPal (Aug. 28, 2019), https://www.eff.org/document/open-letter-venmo.
[73] *Cyber Threats, Consumer Data, and the Financial System: Hearing before the H. Subcomm. on Consumer Prot. and Fin. Inst. of the H. Comm. on Fin. Serv.* (2021) (testimony of Samir Jain, Director of Policy, Center for Democracy & Technology), https://cdt.org/wp-content/uploads/2021/11/hhrg-117-ba15-wstate-CDT-Samir-Jain20211103-House-Financial-Commitee-testimony.pdf.
[74] 15 U.S.C. §1681b.
[75] Justin Sherman, *Federal Privacy Rules Must Get "Data Broker" Definitions Rights*, Lawfare (Apr. 8, 2021, 11:00 AM), https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right.

and lack of transparency with respect to data brokers' practices.[76] According to a new report by researchers at Duke University, data brokers sell people's mental health and medication data as well as non-medical data, grouped into lists such as "Anxiety Sufferers" and "Consumers with Clinical Depression in the United States" to whom advertisements related to their medical needs are targeted.[77] This example demonstrates how the data broker industry has expanded to derive consumer data from a wider network of data sources. California and Vermont have established data broker registries that each surpass five hundred data brokers.[78]

People have little insight into how these profiles are formed and how the data broker network uses this data. Companies that purport to inform people about how their data is shared often bury details about sprawling networks of third parties that receive and use consumer data, within voluminous privacy policies. People do not have to go far to run into data brokers –even internet service providers sell and share online users' data with third parties.[79] For example, Comcast's privacy policy puts the burden on people to opt out of the sharing of non-personally identifiable information, which includes IP addresses and account numbers.[80] AT&T's privacy policy also requires people to opt out of the sharing of people's personal data with affiliates and other companies to deliver advertising and marketing campaigns.[81]

Accountability is difficult to achieve in the data broker network, because the data can be repurposed for uses other than the purpose for which it was previously sold, and certainly for

---

[76] Staff of S. Comm. on Com., Sci., and Transp., 113th Cong., *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (2014), https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577; Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[77] Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Sanford Cyber Policy Program (2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf (explaining that these lists are based on data on people with depression, anxiety, ADHD, insomnia, bipolar, and other mental health disabilities, along with demographic and other non-medical data).

[78] California Department of Justice, https://oag.ca.gov/data-brokers; Vermont Secretary of State, https://bizfilings.vermont.gov/online/DatabrokerInquire/DataBrokerSearch.

[79] Federal Trade Commission, *A Look at What ISPs Know About You: Examining Privacy Practices of Six Major Internet Service Providers* (2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[80] Comcast Xfinity, *Our Privacy Policy Explained* (effective Oct. 12, 2021), https://www.xfinity.com/privacy/policy#privacy-who.

[81] AT&T, *AT&T Privacy Policy* (effective June 6, 2022), https://about.att.com/privacy/full_privacy_policy.html.

uses other than what people reasonably expect based on any insight they do have.[82] People also lack the means to exercise control over how data brokers obtain and sell their data – people often do not have established relationships with data brokers or even know which data brokers are accessing their data. Therefore, people cannot track who shares their data or consent to the collection and use of their data as they would with companies whose goods or services they choose to use. This is complicated further by the fact that the roles of companies that share consumer data have blurred or expanded, leaving people even more uncertain about exactly what data is shared and where. For instance, platforms like Facebook that were once mainly spaces for socializing have grown into spaces for advertising, shopping, and processing financial transactions, while platforms like Venmo that are primarily payment platforms have adopted features of social media.[83]

Third-party data sharing can have even more severe consequences for marginalized communities. For instance, LexisNexis and Thomson Reuters are reportedly among the most prominent data brokers compiling large quantities of personal data to sell to immigration authorities. The compiled data includes publicly available information as well as data from utility companies' records, but reports indicate it is then used to target immigrant communities and punish immigration activists for exercising their rights to free speech and protest.[84] Another example is Verisk, which reportedly sells the data it collects from companies that provide connected home and mobile devices, as well as personally identifying information like phone numbers and addresses, to insurers who use the data to help set rates for insurance products.[85]

Other data brokers take the form of people-search platforms like Spokeo that combine personal data with publicly available data, providing more granular information to users who pay for

---

[82] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, *Legal Loopholes and Data for Dollars* 12 (2021), https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/.

[83] Jack Morse, *Payment Apps Collect and Share Your Data. Here's How to Lock Them Down.*, Mashable (June 9, 2021), https://mashable.com/article/venmo-cash-app-paypal-data-privacy. *See also Comments Regarding CFPB Inquiry Into Big Tech Payment Platforms*, *supra* note 68.

[84] *LexisNexis Illegally Collected and Sold People's Personal Data, Lawsuit Alleges*, CBS News (Aug. 16, 2022, 3:16 PM), https://www.cbsnews.com/news/lexisnexis-lawsuit-collected-sold-personal-data-immigration-advocates-allege/; Max Rivlin-Nadler, *How ICE Uses Social Media to Surveil and Arrest Immigrants*, The Intercept (Dec. 22, 2019, 8:00 AM), https://theintercept.com/2019/12/22/ice-social-media-surveillance/.

[85] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke U. Sanford Cyber Policy Program 6-7 (2021), https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

premium access.[86] When accurate, the resulting information can enable abusers to stalk victims of intimate partner violence, and it can in turn be shared to other websites.[87] When inaccurate, the data may erroneously influence decisions that involve background checks, such as in housing or employment.[88] Spokeo was found to have violated the FCRA when it failed to maintain reasonable procedures to verify the users of its information and whether the use was for a permissible purpose.

The CFPB recently took steps to clarify that the permissible purposes for compiling and furnishing data under the FCRA apply only with respect to the consumer whose data is the subject of the data user's request. The CFPB explained that consumer reporting agencies violate the FCRA when sharing consumer report data of multiple people because the shared data would include people for whom the user did not have a permissible purpose to request the data.[89]

C. Harms of behaviorally targeted advertising to certain audiences based on actual or inferred characteristics

(Questions 1f, 2, 2a, 3, 3b, and 3d)

Behaviorally targeted advertising is used to deliver advertisements to a designated audience based on a range of data, including characteristics about people that represent a particular combination of demographic data and proxies for this data, and behavioral data such as people's online browsing or offline activity. This model of advertising typically depends on extensive commercial surveillance and the easily debunked idea that past behavior accurately forecasts future tendencies. For instance, a person's browsing history is not a very good proxy for future behavior because there are many reasons unrelated to purchase interest that a person would go to a website (misclicked a link, a friend or family member could have been using their device, or no longer be interested in the product or service they browsed).

---

[86] Mara Hvistendahl, *I Tried to Get My Name Off People-Search Sites. It Was Nearly Impossible.*, Consumer Reports (Aug. 20, 2020), https://www.consumerreports.org/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly--a0741114794/.

[87] Kaveh Waddell, *How FamilyTreeNow Makes Stalking Easy*, The Atlantic (Jan. 17, 2017), https://www.theatlantic.com/technology/archive/2017/01/the-webs-many-search-engines-for-your-personal-information/513323/.

[88] Steven Melendez, *When Background Checks Go Wrong*, Fast Company (Nov. 17, 2016), https://www.fastcompany.com/3065577/when-background-checks-go-wrong.

[89] 87 Fed. Reg. 41243.

Behaviorally targeted advertising can cause deep and lasting harms to all people, and most especially to marginalized populations, including psychological and physical harms, unwanted intrusion, discrimination, or unfair manipulation. For instance, a recent study shows that across Facebook, Twitter, Instagram, and TikTok, advertisements and other sponsored content for weight loss products have been targeted to adult people identified as more susceptible to disordered eating.[90] This susceptibility is inferred from data collected about their online activities, such as signals of demographic information, searches for health- or nutrition-related information, and participation in online communities that are related to health or exercise or that encourage disordered eating.[91] These advertisements also tend to be targeted based on data related to gender, which causes the targeted audience to include people whose actual gender identities do not align with the gender norms that inform the parameters designating the audience.[92] This targeting contributes to anxiety, depression, low self-esteem, and physical harms like unhealthy dieting or exercise, or taking pills with harmful side effects.

The use of data collected about someone's online activities makes these harms more persistent and repeated than the more universal encounters of diet culture in broadcast media. The lack of rules to protect people from intrusion related to online activity may also create a chilling effect and discourage people from seeking out information on important but sensitive topics. People increasingly recognize that surveillance is pervasive and hard to control, and regularly report altering their behavior and avoiding seeking out content because of the risks of pervasive tracking and disclosure through online advertising or recommendation systems.[93]

D. Data- and algorithm-driven decision-making used in ways that limit access to critical opportunities

(Questions 1f, 1g, 2, 2a-2c, 3, 3a-3f, and 6d)

---

[90] Liza Gak, Seyi Olojo, & Niloufar Salehi, *The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating*, 1 Assoc. For Computing Mach. 9 (April 2022), https://arxiv.org/pdf/2204.03200.pdf.

[91] *Id.* at 4, 10.

[92] *Id.* at 12.

[93] Nick Doty, *Competing and Collaborating for Better Web Privacy*, Center for Democracy & Technology (Aug. 4, 2022), https://cdt.org/insights/competing-and-collaborating-for-better-web-privacy/; Scott Ikeda, *Study Shows Privacy Awareness is the "New Normal" for People, Online Behavior is Much More Guarded,* CPO Magazine (Nov. 4, 2022), https://www.cpomagazine.com/data-privacy/study-shows-privacy-awareness-is-the-new-normal-for-people-online-behavior-is-much-more-guarded/; DataGrail, *The Great Privacy Awakening (2022),* https://www.datagrail.io/resources/interactive/2022-consumer-privacy-survey/people-take-action-for-privacy-online.

Data- and algorithm-driven decision-making systems influence decisions in multiple critical areas, including housing, credit, employment, and education. People have little to no choice in being subjected to these systems to access the opportunities about which the systems make decisions, and people may not be able to anticipate these systems' harms. Unregulated and inappropriate data use can result in biased training data for AI systems, compound historical discrimination, and yield incorrect assumptions. Unfortunately, all too often, these risks are disproportionately borne by historically marginalized groups, including people of color, immigrants, Indigenous populations, women, people with disabilities, and the LGBTQ+ community.[94]

The resulting harms can take a number of different forms, and can occur for a number of reasons:

- Companies train these systems on data sets that do not accurately represent all people on which the systems are used – or conversely, the training data may incorporate substantial data that overrepresents a particular protected class.
- Companies may design these systems to evaluate consumer data from which protected characteristics could be inferred, which could enable or result in discrimination.
- Companies may not design these systems to ensure that all people subject to the systems can successfully navigate and use them.
- Companies may fail to establish processes for auditing the systems for inaccuracies or biases sufficiently to address and correct all harms.

Note that these factors are not always intentional. System design often executes the priorities and policies of the companies developing and using these systems, as well as societal biases regarding which people are entitled to have their fundamental needs met. In particular, people with a range of different disabilities, including chronic illnesses and mental health disabilities, face significant discrimination by algorithm-driven decision-making systems in a wide swath of areas, both because of exclusionary design and because of discriminatory targeting or profiling. Companies are neglecting disability-specific considerations when their decision-making systems rely on training data and operations parameters that under-represent disabled people, and companies can enable targeting of disabled people when training data and parameters overrepresent disabled people. Yet, the lack of transparency in how these decision-making systems work makes it difficult for people to demonstrate that a data practice has violated current federal civil rights laws.

[94] *See generally* Crawford, *Placing Equity, supra* note 44.

Below, we discuss how companies are misusing data-driven systems in ways that make it difficult for people to challenge the data practice responsible for discriminatory housing, credit, employment, and education decisions.

i. Housing and credit

(Questions 2, 2a, 2b, 2c, 3, 3a, and 3b)

To inform mortgage and other lending decisions and to screen rental applicants, "fintech" companies deploy systems that evaluate credit history, employment and income data, banking and purchase activity, rental payment history, eviction records, arrest and court records, education history, and other data.[95] These data points are supposed to predict whether applicants will fulfill the obligations that come with the housing or loan opportunities for which they are applying. However, many fintech companies' systems have been shown to charge higher interest rates to low-income and Black borrowers, and the systems are not designed to account for the context in which this data is generated.[96]

For instance, data about past arrest records, eviction proceedings, and financial, employment, and education history may not reflect people's *current* ability to make regular rental payments or loan repayments.[97] Meanwhile, data that would more reliably indicate current ability to make regular payments, such as recent history of on-time utility payments, is not considered.[98] As a result, people can remain trapped in a cycle of poor access to credit because they are punished for past records despite changes in their circumstances or qualifications. In addition, tenant screening companies like CoreLogic use algorithms that consider data such as arrest and

---

[95] Jung Choi, Karan Kaul, & Laurie Goodman, *FinTech Innovation in the Home Purchase and Financing Market*, Urban Inst. 9 (2019), https://www.urban.org/sites/default/files/publication/100533/fintech_innovation_in_the_home_purchase_and_financing_market_2.pdf; Karen Hao, *The Coming War on The Hidden Algorithms That Trap People in Poverty*, MIT Tech. Rev. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back/.

[96] Choi et al., *supra* note 95, at 10-11.

[97] Christopher K. Odinet, *The New Data of Student Debt*, 92 Southern Cal. L. Rev 1617, 1667 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3349478; Center for Democracy & Technology, Comments to Financial Regulators on Financial Institutions' Use of Artificial Intelligence, Jul. 1, 2021, https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf.

[98] *Id.* at 1663; Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage Approval Algorithms*, The Markup (Aug. 25, 2021, 6:50 AM), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

eviction records, which are unreliable predictors for how applicants will treat other tenants or property.[99] Higher volumes of arrest data are generated in overpoliced neighborhoods, disproportionately affecting Black, Indigenous, and Latinx communities, disabled people, and transgender people. Landlords often evict tenants after calls to police related to domestic violence – as CDT has written, this occurs even more frequently for disabled people and people of color, and contributes to unreliable eviction data.[100]

Biometric data can also contribute to housing decisions. Besides tenant screening and other functions, property technology companies also provide video surveillance and facial recognition to monitor properties for any unpermitted activity or unauthorized presence, and biometric entry systems to prevent such situations.[101] In these cases, biometric data can also trigger evictions or arrests, further criminalizing people who are already disproportionately surveilled, and for whom facial analysis has been shown to produce unreliable matches.[102] Disabled people are currently at extraordinary risk of compounded discriminatory effects of rapidly expanding surveillance technologies. For instance, studies estimate up to 85% of incarcerated youth have learning or behavioral disabilities.[103] Use of tenant screening software, employment background checks, and predictive policing tools that inappropriately and sometimes illegally use arrest or conviction records thus has an outsized impact on disabled people, creating further inequities down the line in access to housing, employment, and social services.

Housing discrimination also occurs through behaviorally targeted advertising, which has been shown to direct advertisements for critical opportunities and services to, or away from, certain

---

[99] Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Center for Democracy & Technology (July 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/ [hereinafter Brown, *Tenant Screening Algorithms*].

[100] Am. Civ. Liberties Union, *Calling 911 Shouldn't Lead to an Eviction* (Mar. 15, 2022, 1:45 PM), https://www.aclu-wi.org/en/news/calling-911-shouldnt-lead-eviction.

[101] Avi-Asher Schapiro, *Good Business or Digital Bias? The Divisive Rise of 'Proptech',* Thomson Reuters (July 15, 2020, 5:14 PM), https://news.trust.org/item/20200715162819-bngcy; Anti-Eviction Mapping Project, Landlord Tech Watch, https://antievictionmappingproject.github.io/landlordtech/.

[102] *See generally* Sophia Maalsen, Peta Wolifson, Dallas Rogers, Jacqueline Nelson, and Caitlin Buckle, AHURI, *Understanding Discrimination Effects in Private Rental Housing* (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916655. *See also* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings Of Machine Learning Research 2 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[103] Daja E. Henry & Kimberly Rapanut, *How Schools and the Criminal Justice System Both Fail Students with Disabilities*, Slate (Oct. 21, 2020, 9:00 AM), https://slate.com/news-and-politics/2020/10/students-disabilities-criminal-justice-system.html.

categories of people who would be interested in acting on the advertisements. In such cases, targeted advertising can either deny these people access to information that could help them access opportunities and services, or relegate them to receiving advertisements for more unfavorable opportunities or products.[104] For example, a Department of Justice (DOJ) lawsuit alleged that Meta's advertising system enabled advertisers to use categories created based on race, color, religion, sex, disability, familial status, and national origin, and proxies for these characteristics, to designate eligible audiences for delivery of housing advertisements.[105]

While the companies responsible for data-driven discrimination in lending and housing should be subject to liability under federal civil rights laws, the lack of transparency from companies erects barriers for people to vindicate their civil rights even against entities that are subject to civil rights laws. The Fair Housing Act (FHA) prohibits discrimination in advertisements, offers, and sale or rental of housing on the basis of race, color, religion, sex, disability, familial status, or national origin.[106] The Department of Housing and Urban Development (HUD) has warned that the use of criminal arrest records can violate the FHA because it can have a disparate impact based on race and national origin.[107] HUD has also advised that evictions following domestic violence-related calls to police can indicate disability or gender discrimination,[108] which can make housing decisions relying on eviction records more likely discriminatory as well. This has not deterred the use of tenant screening algorithms that include these records, though.[109]

HUD and other agencies have initiated efforts to address the ongoing harms of tenant screening algorithms. The CFPB published reports last fall examining the prevalence of tenant screening platforms and their impacts on housing access for marginalized renters, observing that while

---

[104] *See e.g.*, Julia Angwin & Terry Parris, Jr., *Facebook Says It Will Stop Allowing Some Advertisers to Exclude Users by Race*, ProPublica (Nov. 11, 2016, 10:00 AM), https://www.propublica.org/article/facebook-to-stop-allowing-some-advertisers-to-exclude-users-by-race.

[105] Department of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

[106] 42 U.S.C. §3604 *et seq*.

[107] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions* (2016), https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.

[108] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Enforcement of Local Nuisance and Crime-Free Housing Ordinances Against Victims of Domestic Violence, Other Crime Victims, and Others Who Require Police or Emergency Services* (2016) https://www.hud.gov/sites/documents/FINALNUISANCEORDGDNCE.PDF.

[109] Brown, *Tenant Screening Algorithms*, *supra* note 99.

these tools can violate fair housing and consumer protection laws, renters are unable to dispute adverse outcomes arising from these tools.[110] HUD recently announced that it will issue guidance regarding how tenant screening algorithms can violate the FHA, and will work with the FTC, CFPB, and other agencies to release best practices for using tenant screening reports.[111] And the FTC and CFPB have since issued a request for information on tenant screening issues affecting the public, including the role of algorithm-based systems on these issues.[112]

The Equal Credit Opportunity Act (ECOA) prohibits discrimination against applicants in any aspect of a credit transaction on the basis of race, color, religion, national origin, sex, marital status, age, or income derived from a public assistance program.[113] The CFPB issued guidance in 2022 stating that the ECOA requires creditors to provide people with a specific and accurate statement of principal reasons for adverse actions resulting from an algorithmic system.[114] Data practices that make or inform decisions regarding the extension of credit can violate the ECOA by using data that functions as proxies for these protected characteristics, but this does not extend to disability discrimination.

The ECOA requires creditors to inform credit applicants in writing about the reasons for an adverse credit decision or about the applicants' right to receive such a notice upon request, including for adverse actions resulting from algorithmic systems.[115] CDT has raised concerns about this form of notice to financial regulators, observing that it does not give applicants an opportunity to verify the accuracy of the data being evaluated during the approval process, or to provide additional information to supplement that data.[116] The ECOA also requires correction of inaccuracies in credit records upon request, which places responsibility on people to detect such errors, without clarity about which data contributed to the ultimate decision. Further, the

---

[110] *CFPB Reports Highlight Problems with Tenant Background Checks*, Nov. 15, 2022, https://www.consumerfinance.gov/about-us/newsroom/cfpb-reports-highlight-problems-with-tenant-background-checks/.
[111] The White House Blueprint for a Renters Bill of Rights (2023), https://www.whitehouse.gov/wp-content/uploads/2023/01/White-House-Blueprint-for-a-Renters-Bill-of-Rights.pdf.
[112] Federal Trade Commission, *FTC and CFPB Seek Public Comment on How Background Screening May Shut Renters Out of Housing* (Feb. 28, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-cfpb-seek-public-comment-how-background-screening-may-shut-renters-out-housing.
[113] 15 U.S.C. §1691(a).
[114] Consumer Financial Protection Bureau, *Circular 2022-03: Adverse Action Notification Requirements in Connection With Credit Decisions Based on Complex Algorithms*, https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.
[115] *Id.*; 15 U.S.C. §1691(d)(2).
[116] Samir Jain & Ridhi Shetty, *Taking a Hard Line on AI Bias in Consumer Finance*, Center for Democracy & Technology, https://cdt.org/insights/taking-a-hard-line-on-ai-bias-in-consumer-finance/.

ECOA offers limited recourse for targeted advertising – it protects people who actually apply for credit, extending to prospective applicants only insofar as it prohibits creditors from stating discriminatory preferences in advertising.[117]

ii. Employment

(Questions 2, 2a, 2b, 2c, 3, 3a, and 3b)

Algorithmic tools play a driving role in decisions including hiring, promotion, and termination. Vendors develop hiring technologies that aim to distinguish candidates in an applicant pool based on attributes they appear to have in common with other successful candidates and employees – in other words, attributes of people who have historically been hired more often.[118] Vendors market many of these tools as bias audited or less biased, without showing how (or even whether) the tools have been examined for disability bias.[119] Meanwhile, the tools collect and analyze data about candidates that is not relevant to candidates' ability to perform job functions, causing workers to be rejected over irrelevant data related to marginalized identities.[120]

One such algorithm-driven hiring tool is resume screening. Ideal's resume screening software analyzes language and details in resumes, from candidates' names to affiliations to employment gaps, to identify whether the resumes reflect qualities the tools are designed to look for.[121] Taleo assigns bonus points for keywords in resumes that reflect attributes that are desired but

---

[117] 12 C.F.R. Supplement I to Part 1002, Paragraph 4(b).

[118] Miranda Bogen & Aaron Rieke, Upturn, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* (2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

[119] *See* Manish Raghavan, Solon Barocas, Jon Kleinberg, & Karen Levy, *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 469 (2020), https://arxiv.org/pdf/1906.09208.pdf.

[120] *See* Hilke Schellmann, *Finding it Hard to Get a New Job? Robot Recruiters Might Be to Blame*, The Guardian (May 11, 2022, 4:30 PM), https://www.theguardian.com/us-news/2022/may/11/artitifical-intelligence-job-applications-screen-robot-recruiters (discussing how automated hiring technologies exhibit gender biases and use criteria such as names and data about non-professional activities).

[121] Ideal, *Screening*, https://ideal.com/product/screening/. *See also* Avi-Asher Schapiro, *AI is Taking Over Job Hiring, But Can it Be Racist?*, Thomson Reuters (Jun. 7, 2021, 7:04 AM), https://www.reuters.com/article/global-tech-ai-hiring/analysis-ai-is-taking-over-job-hiring-but-can-it-be-racist-idUSL5N2NF5ZC.

not required.[122] As Amazon's now-discontinued resume screening tool demonstrated, resume screening tools can observe patterns in resumes that are moved forward in the hiring process and learn to filter out resumes with terms associated with women, such as women-oriented affiliation groups.[123] Such tools could similarly learn to exclude candidates based on data related to racial or ethnic identity.[124] Additionally, marginalized people who have previously experienced discrimination in their education, employment, or access to healthcare (especially if they face multiple forms of discrimination) might not get past screening tools that downgrade or screen out resumes before human reviewers can consider them. For instance, a disabled person may previously have had difficulty getting full-time employment, thus leading to gaps in their resume that will be flagged by such systems.[125]

Research by CDT and fellow advocates has raised concerns about other tools that purport to measure "soft skills" through gamified personality and aptitude assessments, or through analysis of video interviews.[126] The use of such tools presumes that everyone demonstrates the traits employers look for – such as empathy, optimism, or adaptability – the same way. Paradox Traitify provides candidates with a series of images, requiring them to indicate whether they identify with what is depicted in each image to determine their alignment with a pseudoscientific personality model.[127] Pymetrics analyzes data collected while candidates complete a set of games to predict "cognitive and emotional attributes," which it claims to be "fairness-optimized" but has not been examined for disability bias.[128] Pymetrics was recently

---

[122] James Hu, *Taleo: 4 Ways the Most Popular ATS Ranks Your Job Application*, Jobscan (Mar. 8, 2018), https://www.jobscan.co/blog/taleo-popular-ats-ranks-job-applications/.

[123] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women,* Thomson Reuters (Oct. 10, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[124] Rachel Goodman, *Why Amazon's Automated Hiring Tool Discriminated Against Women*, American Civil Liberties Union (Oct. 12, 2018), https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against.

[125] Jim Fruchterman & Joan Mellea, Benetech, *Expanding Employment Success for People With Disabilities* (2018), https://benetech.org/about/resources/expanding-employment-success-for-people-with-disabilities-2/.

[126] Center for Democracy & Technology, *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?* 11-12 (2020), https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf; Aaron Rieke, Urmila Janardan, Mingwei Hsu, and Natasha Duarte, Upturn, *Essential Work* (2021), https://www.upturn.org/work/essential-work/.

[127] Paradox, *Assessments*, https://www.paradox.ai/products/assessments; Olivia Goldhill, *We Took the World's Most Scientific Personality Test – and Discovered Unexpectedly Sexist Results* (Feb. 11, 2018), https://qz.com/1201773/we-took-the-worlds-most-scientific-personality-test-and-discovered-unexpectedly-sexist-results/.

[128] Pymetrics, *Assessments*, https://www.pymetrics.ai/assessments; Christo Wilson, Avijit Ghosh, Shan Jiang, Alan Mislove, Lewis Baker, Janelle Szary, Kelly Trindel, and Frida Polli, *Building and Auditing Fair Algorithms: a Case Study in Candidate Screening* (2021), https://evijit.github.io/docs/pymetrics_audit_FAccT.pdf.

acquired by Harver, which implements "behavioral-based AI methodology" in soft skills assessments and automates matching of "high-potential" candidates.[129] Cappfinity's Koru uses a survey that requires candidates to select the responses with which they feel they align most, to assess soft skills.[130] Blind people and people with mobility impairments might not be able to adequately interface with a gamified assessment, while people with mental health disabilities or cognitive disabilities might have difficulty processing the information quickly enough to score well. Similarly, autistic and other neurodivergent people may be unable to answer correctly on personality tests that score candidates on characteristics unrelated to core competencies or essential functions of the job at hand.

HireVue has used video interview assessments that process data about how candidates physically appear, move, emote, and sound as they respond to interview questions. This treats candidates' eye contact, facial expressions, fidgeting, tics, vocabulary, and speech patterns as data points to infer personality traits such as confidence and trustworthiness.[131] HireVue has stated that it does not use video analysis or audio characteristics, but it analyzes personality traits and aptitudes by applying natural language processing to a transcription developed through an AI-driven speech-to-text service.[132] Disabled candidates who possess the traits that are necessary for successful job performance can nonetheless be scored unfairly by this type of tool, because their disabilities can cause them to demonstrate examined traits in ways that cannot be accurately captured through the analyzed data points.[133] This type of tool could also produce unfair scores for candidates of color or candidates who have been socialized to follow certain gender norms, as cultural norms can also affect speech patterns and eye contact.[134] HireVue also claims its product has been audited for fairness, but does not make its audit report available unless one provides their name, email address, and professional affiliation and agrees

[129] Harver, *Harver Acquires Pymetrics, Further Enhancing Talent Decision Capabilities Across the Employee Lifecycle* (Aug. 11, 2022), https://harver.com/press/harver-acquires-pymetrics/; Harver, *Assessments*, https://harver.com/software/assessments/; Harver, *Hiring Process Optimization*, https://harver.com/software/hiring-process-optimization/.
[130] Cappfinity, *Skills Identification*, https://www.cappfinity.com/cappfinity-product-page/assessment-cognitive-3/.
[131] Drew Harwell, *A Face-Scanning Algorithm Increasing Decides Whether You Deserve the Job*, Wash. Post (Nov. 6, 2019, 12:21 PM), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.
[132] HireVue, *Explainability Statement* (2022), https://webapi.hirevue.com/wp-content/uploads/2022/03/HV_AI_Short-Form_Explainability_3152022.pdf.
[133] Matthew Scherer, *HireVue "AI Explainability Statement" Mostly Fails to Explain what it Does*, Center for Democracy & Technology (Sept. 8, 2022), https://cdt.org/insights/hirevue-ai-explainability-statement-mostly-fails-to-explain-what-it-does/.
[134] Goodman, supra note 124.

not to use any part of the audit report without HireVue's written authorization.[135] HireVue is now facing a class action lawsuit over its collection and use of biometric data.[136]

Companies are also increasingly developing and deploying sophisticated electronic surveillance to automate the monitoring and management of workers, whether they are in a warehouse, out making deliveries, at an office, or working remotely from home. CDT's report, *Warning: Bossware May Be Hazardous to Your Health*, examines companies' use of such automated systems, commonly referred to as "bossware," to perform a wide variety of monitoring tasks, such as tracking workers' location and movements, productivity and downtime, computer use, facial expressions, biometric markers, and frequency and length of bathroom and other breaks.[137] One system, Crossover's WorkSmart productivity tool, takes periodic screenshots and images of workstations to monitor what workers are doing.[138] Another company, Time Doctor, prevents workers from deleting screenshots to protect their privacy by deducting time worked during the period when screenshots were taken.[139] Some programs use workers' phones or computers to listen, watch, or monitor other sensors in their device, and can penalize workers for moving away from their workstation or slowing productivity.

Companies often use these technologies to optimize tasks for their own profit, but they put workers' health and safety at risk and threaten their privacy, autonomy, and dignity.[140] For example, Amazon has used productivity monitoring to monitor "time off task," which triggers warnings to workers for resting even when needed, putting them at risk of termination if they

---

[135] HireVue, *Download IO Psychology Audit Description by Landers Workforce Science LLC*, https://www.hirevue.com/resources/template/hirevue-io-psychology-audit-report.

[136] Samantha Hawkins, *HireVue Attempts to Escape Biometrics Suit Over AI Interviews*, Bloomberg (June 22, 2022, 1:16 PM), https://news.bloomberglaw.com/privacy-and-data-security/hirevue-attempts-to-escape-biometrics-suit-over-ai-interviews.

[137] Jodi Kantor, Arya Sundaram, Aliza Aufrichtig, & Rumsey Taylor, *Workplace Productivity: Are You Being Tracked?*, N.Y. Times (Aug. 16, 2022, 10:03 AM), https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html; Spencer Soper, *Fired by Bot at Amazon: 'It's You Against the Machine'*, Bloomberg (June 28, 2021, 6:00 AM), https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out.

[138] Sean Captain, *In 20 Years, Your Boss May Track Your Every Glance, Keystroke, and HeartBeat*, Fast Company (Jan. 27, 2020), https://www.fastcompany.com/90450122/in-20-years-your-boss-may-track-your-every-glance-keystroke-and-heartbeat.

[139] Matt Scherer, Center for Democracy & Technology, *Warning: Bossware May Be Hazardous to Your Health* 9 (2021), https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/ [hereinafter *Bossware*].

[140] *Id.* at 36.

do not work at a pace that is dangerously fast.[141] Productivity monitoring also fails to capture work that is being performed offline or that cannot be accurately quantified through surveillance measures, and can punish and deter worker organizing.[142]

Many low-wage and hourly workers endure constant surveillance, often combined with algorithmic management systems that can discipline or even terminate them.[143] This exacerbates the already-wide gaps in information and bargaining power that low-wage workers face. Algorithmic tools further diminish gig workers' bargaining power, as they determine compensation and availability and termination of jobs.[144]

Low-wage workers marginalized on the basis of disability, race, ethnicity, and gender identity are at an even greater disadvantage. As many as 100,000 disabled workers are paid subminimum wages due to a provision in the Fair Labor Standards Act that allows employers to pay disabled workers commensurate with wages paid to non-disabled workers for "the same type, quality, and quantity of work" – effectively limiting disabled workers' wages based on their challenges in meeting productivity expectations.[145] In other words, this provision allows an employer to pay a disabled worker only for the hours a non-disabled worker would take to complete the same work rather than the hours of labor the disabled worker has actually put in. Productivity monitoring systems can discriminate against disabled workers, pregnant or breastfeeding workers, older workers, and workers requiring religious prayer breaks by flagging breaks or slower pace of work, increasing the risk of injury to physical or mental health.[146] These

---

[141] Deborah Berkowitz, *Packaging Pain: Workplace Injuries in Amazon's Empire*, Nat'l Emp. Law Project, https://www.nelp.org/publication/packaging-pain-workplace-injuries-amazons-empire/; Colin Lecher, *How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity'*, The Verge (Apr. 25, 2019, 12:06 PM), https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

[142] Kantor et al., *supra* note 137.

[143] Aiha Nguyen, *The Constant Boss: Labor Under Digital Surveillance*, Data & Society (2021), https://datasociety.net/library/the-constant-boss/.

[144] Federal Trade Commission, Policy Statement on Enforcement Related to Gig Work (Sept. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Matter%20No.%20P227600%20Gig%20Policy%20Statement.pdf.

[145] Rebecca Vallas, Kim Knackstedt, Hayley Brown, Julie Cai, Shawn Fremstad, & Andrew Stettner, The Century Fdn. and Disability Econ. Just. Collaborative, *Economic Justice is Disability Justice* (2022), https://tcf.org/content/report/economic-justice-disability-justice/. Section 14(c) of the Fair Labor Standards Act allows employers to apply for special certificates to employ disabled workers at subminimum wages. 29 U.S.C. §214(c).

[146] *The Future of Work: Protecting Workers' Civil Rights in the Digital Age, Before House Comm. on Ed. & Labor, Civil & Human Serv. Subcomm.* (2020) (testimony of Jenny Yang, Senior Fellow, Urban Institute), https://edlabor.house.gov/imo/media/doc/YangTestimony02052020.pdf.

effects are especially worse for people with physical, mental health, developmental, or cognitive disabilities.

Relatedly, more employers are relying on workplace wellness programs to increase worker productivity while reducing the cost of benefits claims for employers, even turning to gamified approaches to influence employees' behavior and personal health decisions.[147] Studies have shown that these programs do not deliver the intended positive effects on healthcare expenses or productivity.[148] Meanwhile, the programs impose expectations for physical exercise and diet that disabled workers may not be able to meet, and reinforce the higher societal value assigned to being "healthy."[149] To make matters worse, these programs pressure employees to provide health data that might make its way to third parties.[150]

While the discriminatory outcomes of hiring and algorithmic management technologies run afoul of federal employment discrimination laws, enforcement has not kept up with these technologies. For instance, Title I of the ADA prohibits adverse employment decisions based on workers' disability, and it requires employers to provide reasonable accommodations when doing so would not pose an undue hardship on employers.[151] Hiring and algorithmic management technologies provided by private companies can make or influence adverse decisions using disability-related data, without informing workers about how the technologies are collecting and analyzing their data, how this will influence employment decisions, and how workers might access accommodations that enable fairer evaluation.[152] Thus, workers may not have enough detail to pursue disability discrimination claims arising from these technologies' use. Similar issues plague enforcement of Title VII of the Civil Rights Act. The Equal Employment Opportunity Commission's draft Strategic Enforcement Plan for Fiscal Years 2023-2027

[147] *See* Joseph Sanford & Kevin Sexton, *Opinion: Improve Employee Health Using Behavioral Economics*, CFO (Feb. 3, 2022), https://www.cfo.com/human-capital/health-benefits/2022/02/employee-health-wellness-medical-claims-behavorial-economics/.
[148] Sally Wadyka, *Are Workplace Wellness Programs a Privacy Problem?*, Consumer Reports (Jan. 16, 2020), https://www.consumerreports.org/health-privacy/are-workplace-wellness-programs-a-privacy-problem-a2586134220/.
[149] Brown, *Surveillance Technologies*, *supra* note 4, at 54-55; Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance*, 129-30, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211.
[150] *Id.*
[151] 42 U.S.C. §12112.
[152] *Algorithm-Driven Hiring Tools*, *supra* note 126.

recognizes these issues, and the agency plans to dedicate resources to addressing employment discrimination related to the use of algorithm-driven hiring technologies.[153]

Beyond civil rights protections, there are few other laws or rules governing employers' use of surveillance technologies or safeguarding workers from their harmful effects. Workers have no concrete privacy rights under either federal law or the laws of most states. The Occupational Safety and Health Act prohibits practices that pose a risk of death or serious injury to workers, but the Occupational Safety and Health Administration's regulations do not cover many of the harms to workers' health that these technologies can impose, such as repetitive motion injuries and threats to workers' mental health. Gig workers are also not adequately protected under existing civil rights laws and the Occupational Health and Safety Act, which do not classify all workers as covered "employees."[154]

In addition, a new fact sheet from the Department of Labor regarding reporting requirements under the Labor-Management Reporting and Disclosure Act states that employers must report expenditures made for surveillance of employees and unfair labor practices, but only when the surveillance is used to obtain information connected to a labor dispute or the labor practices are intended to undermine the right to organize.[155]

iii. Education

(Questions 2, 2a, 2b, 2c, 3, 3a, and 3b)

Public sector services, from education to governmental benefits, regularly involve the collection of personal data. Students and families may be subjected to data practices that worsen inequity throughout the education context, from the use of cameras equipped with computer vision on campus, to algorithms that make critical decisions about students' lives, to software that monitors everything students do online — often through technology sold by private contractors. Those uses of data and technology surveil students often without meaningful consent or

[153] Center for Democracy & Technology, *CDT Comments Supporting EEOC's Recognition of Discriminatory Tech as an Enforcement Priority*, Feb. 9, 2023, https://cdt.org/insights/cdt-comments-supporting-eeocs-recognition-of-discriminatory-tech-as-an-enforcement-priority/.

[154] Scherer, *Bossware*, *supra* note 139, at 16.

[155] Jeffrey Freund, *How We're Ramping Up Enforcement of Surveillance Reporting*, Department of Labor Blog (Sept. 15, 2022), https://blog.dol.gov/2022/09/15/how-were-ramping-up-our-enforcement-of-surveillance-reporting; Office of Labor-Management Standards, U.S. Department of Labor, *OLMS Fact Sheet on Form LM-10 Employer Reporting: Transparency Concerning Persuader, Surveillance, and Unfair Labor Practices Expenditures*, https://www.dol.gov/sites/dolgov/files/OLMS/regs/compliance/LM10_FactSheet.pdf.

opportunity to opt out because they are a condition for students' ability to access a fundamental service — their education.

CDT has researched student activity monitoring software, a type of school surveillance technology that allows schools to view students' screens, record their browsing and search histories, and scan their messages and documents stored online or on school devices.[156] The results showed that surveillance is pervasive: 89 percent of teachers report that their school uses student activity monitoring software,[157] and monitoring often occurs even outside of school hours. Although vendors claim that student activity monitoring and other forms of commercial surveillance benefit students, those claims are largely unsubstantiated.[158] Instead, monitoring violates rights traditionally protected by civil rights laws.[159] Further, students experiencing poverty and students of color rely more heavily on school-issued devices, which are more likely to be subject to monitoring than personal devices.[160] As a result, these groups of students are similarly subject to increased risks of discrimination. These incursions on students' fundamental rights are a betrayal of schools' role as "the nurseries of democracy."[161]

National reporting has also underscored the harms caused by commercial surveillance in education. Students with disabilities are at higher risk of generating false positives and false

---

[156] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: The Misleading Promise of Monitoring Students Online* (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of- monitoring-students-online [hereinafter *Hidden Harms*].

[157] *Id.* at 8.

[158] Center for Democracy & Technology & Brennan Center for Justice, Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns (2019), https://cdt.org/insights/social-media-monitoring-in-k-12-schools-civil-and-human-rights-concerns; *see also* Rebecca Heilweil, *The Problem with Schools Turning to Surveillance After Mass Shootings*, Vox (June 2, 2022, 7:30 AM), https://www.vox.com/recode/23150863/school-surveillance-mass-shooting- texas-uvalde; Lucas Ropek, *Surveillance Tech Didn't Stop the Uvalde Massacre*, Gizmodo (May 27, 2022), https://gizmodo.com/surveillance-tech-uvalde-robb-elementary-school-shootin-1848977283; Jolie McCollough & Kate McGee, *Texas Already "Hardened" Schools. It Didn't Save Uvalde.*, Texas Tribune (May 26, 2022), https://www.texastribune.org/2022/05/26/texas-uvalde-shooting-harden-schools;

[159] *Hidden Harms*, *supra* note 156, at 19-24.

[160] DeVan L. Hankerson Madrigal, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman, & Dhanaraj Thakur, Center for Democracy & Technology, *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software* 10 (Sept. 21, 2021), https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/; Hugh Grant-Chapman & Elizabeth Laird, Center for Democracy & Technology, *Research Slides: Key Views Toward Ed Tech, School Data, and Student Privacy* 48 (Nov. 15, 2021), https://cdt.org/insights/report-navigating-the-new-normal-ensuring-equitable-and-trustworthy-edtech-for-the-future.

[161] Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2046 (2021).

negatives when surveilled by student monitoring tools that are designed to identify atypical sounds, text, speech, or movements as potential indicators that students may be engaging in violent or prohibited conduct, making threats, or cheating on tests. For instance, a ProPublica investigation found that aggression-detection microphones were so unreliable that they flagged loud laughter and locker doors slamming as indicators of violence.[162] Those false positives raise concerns for students whose disabilities affect their speech and movement, such as students with cerebral palsy who might not be able to modulate voice volume or students with Tourette's who have loud vocal tics.

Meanwhile, student advocacy organizations such as the National Disabled Law Students Association have documented the discriminatory barriers that students with a wide range of disabilities, including ADD, blindness, and Crohn's disease, experience when required to use automated proctoring software.[163] Students reported not being permitted to take enough bathroom breaks, worrying about false positives from needing to move or pace, or not moving their eyes or hands the right way. For disabled students of color or LGBTQ+ students with disabilities, who also face additional discrimination and prejudice, the risks of student monitoring and commercial surveillance programs are further compounded by their intersected identities.

Although existing laws address many of the impacts of the uses of data and technology on civil rights, they do not cover all harms to historically marginalized groups of people who are not recognized as a legally protected class, such as unhoused students, low-income students, foster care students, and rural students. Title VI[164] and Title IX[165] of the Civil Rights Act prohibit discrimination on the basis of race, sex, and related classes by entities receiving certain federal funds, including in the education sector. However, when discrimination is caused by technology distributed by private contractors for schools, students and families may not be aware of the discriminatory impact, due to a lack of transparency around the implementation and utilization of technological systems. Schools have very little ability to gain insight into contractors' data practices, no matter how reasonable their precautions, and this prevents them from providing parents with adequate notice. Schools, families, and students are consequently dependent on

[162] Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.
[163] National Disabled Law Students Association, *Report on Concerns Regarding Online Administration of Bar Exams* (2020), https://ndlsa.org/wp-content/uploads/2020/08/NDLSA_Online-Exam-Concerns-Report1.pdf.
[164] 42 U.S. Code § 2000d.
[165] 20 U.S.C. §§ 1681–1688.

contractors' representations regarding data use, and need transparency regarding contractors' collection and use of student data.

Students and families do not have a meaningful choice in whether to consent to the surveillance. Students are often required or encouraged to use school-issued devices that are subject to monitoring,[166] or they may rely on school-issued devices because of their families' socioeconomic status.[167] Further, students and families are often not provided accurate, complete disclosures around commercial surveillance in education. For example, in recent CDT research, 47 percent of parents reported they were not informed about how their schools' contractors collect data about students' activity online; only 39% reported they were asked for input on those practices.[168] Even if students and families are provided adequate disclosures, they are typically not given a choice (whether opt-in or opt-out) with respect to whether and how schools or their contractors monitor student online activity. Moreover, it may be impractical or even impossible for students and families to switch schools to avoid their commercial surveillance practices.

For example, an algorithmic system used to assign students to schools may rely on a variety of factors, not all of which may be known to students and families.[169] This information asymmetry may make it difficult or impossible to challenge discriminatory practices caused by data or technology use. In interviews, school IT leaders stated they took strides through contractual measures to hold contractors accountable for their uses of student data, and expressed frustration with "what they describe as a lack of distinguishable options for privacy-forward devices."[170] Similarly, 94 percent of parents and 88 percent of students stated it was "important" for schools to engage them on the uses of student data.[171]

---

[166] Hankerson Madrigal et al., *supra* note 160, at 10.
[167] *Id.*
[168] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: Research Slide Deck* 30–32 (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online.
[169] Hannah Quay-de la Vallee & Natasha Duarte, Center for Democracy & Technology, *Algorithmic Systems in Education* 8-9 (2019), https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/.
[170] Hankerson Madrigal et al., *supra* note 160, at 17.
[171] *Hidden Harms*, *supra* note 156, at 18.

Title VI[172] and Title IX[173] prohibit entities receiving certain federal funds from acquiring discriminatory technology, but would not preclude private vendors from selling it in the first place. Further, certain uses of data and technology may not intentionally discriminate against people based on race, sex, disability status, or other protected classes, but nonetheless cause disparate impact. Courts, however, have curtailed people's ability to challenge disparate impact under critical civil rights laws in court,[174] limiting their ability to seek redress. CDT has called on the Office for Civil Rights in the U.S. Department of Education to address harms from some uses of data and technology on students of color, students with disabilities, and LGBTQ+ students.[175]

Lax data security practices by private contractors in the education sector also cause harm by undermining students' and families' trust in schools and contractors and putting their financial and physical wellbeing at risk. Lax data security practices can result in breaches and other data security incidents, which have substantially increased in both number and scope since 2016 and strained schools' resources.[176] For example, one recent incident involved a contractor serving schools in six states, affecting over three million current and former students.[177] Similarly, a recent ransomware attack on Los Angeles Unified School District resulted in the release of students' personal information, and parents and students have questioned the district's preparation and transparency.[178] A ransomware attack on a Texas school district cost more than

[172] 42 U.S. Code § 2000d.
[173] 20 U.S.C. §§ 1681–1688.
[174] *E.g.*, Jackson v. Birmingham Bd. of Educ., 544 U.S. 167, 178, 178 n.2 (2005) (Title IX); Alexander v. Sandoval, 532 U.S. 275 (2001) (Title VI); Doe v. BlueCross BlueShield of Tenn., Inc., 926 F.3d 235, 240-42 (6th Cir. 2019).
[175] Center for Democracy & Technology, *Comment on Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance*, Docket No. ED-2021-OCR-0166 (filed Sept. 12, 2022), https://cdt.org/insights/cdt-urges-us-department-of-education-to-protect-lgbtqi-students-from-discrimination-in-proposed-title-ix-rules; Letter to Catherine Lhamon, Assistant Secretary for Civil Rights, U.S. Department of Education, from Coalition of Civil, Digital, and Education Rights Organizations (filed Aug. 2, 2022), https://cdt.org/insights/letter-to-ed-office-for-civil-rights-on-discriminatory-effects-of-online-monitoring-of-students/; Center for Democracy & Technology, *Comments on Request for Information Regarding the Nondiscriminatory Administration of School Discipline*, Docket No. ED-2021-OCR-0068 (filed July 23, 2022), https://cdt.org/insights/cdt-comments-to-us-dept-of-ed-urging-the-protection-of-students-of-color-and-students-with-disabilities-and-their-data; Center for Democracy & Technology, *Comments on Announcement of Public Hearing; Title IX of the Education Amendments of 1972*, 86 Fed. Reg. 27429 (filed June 11, 2021), https://cdt.org/insights/cdt-comments-on-protecting-privacy-rights-and-ensuring-equitable-algorithmic-systems-for-transgender-and-gender-non-conforming-students/.
[176] K12 SIX, State of K-12 Cybersecurity 3 (2022), https://www.k12six.org/the-report.
[177] Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022), https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire/.
[178] Howard Blume & Alejandra Reyes-Velarde, *Student Information Remains at Risk After Massive Cyberattack on Los Angeles Unified*, Los Angeles Times (Sept. 7, 2022), https://www.latimes.com/california/story/2022-09-07/

a half million dollars to mitigate, and attacks in Baltimore and Buffalo cost in excess of $9 million each.[179]

As the Government Accountability Office has described, student data "can be sold on the black market and can cause significant financial harm to students who typically have clean credit histories and often do not inquire about their financial status until adulthood."[180] One breach included the personal information of students who completed surveys on bullying, and another included students' phone numbers, which "were used to send text messages that threatened physical violence."[181] In light of these harms, "COPPA-covered companies, including ed tech providers, must have procedures to maintain the confidentiality, security, and integrity of children's personal information. For example, even absent a breach, COPPA-covered ed tech providers violate COPPA if they lack reasonable security."[182]

Policymakers should note that public sector services are provided in part or entirely by private contractors or vendors, so new regulations should protect the privacy-forward provision of governmental services by such contractors.[183] Governments regularly contract out services to private companies, and many of those services involve data collection and use. Schools and school districts may contract with private contractors to provide systems for online lessons, communications services, or managing students' personal information. Other governmental entities may contract with private entities for a variety of services such as identity verification. A

---

los-angeles-unified- schools-cyberattack; Joshua Bay, *LA Parents Sound Off After Cyberattack Leaves Students Vulnerable*, The 74 (Oct. 7, 2022), *https://www.the74million.org/article/la-parents-sound-off-after-cyberattack-leaves-students-vulnerable*.

[179] K12 SIX, *supra* note 176, at 8; *see also* McKenna Oxenden, *Baltimore County Schools Suffered a Ransomware Attack. Here's What You Need to Know*, Baltimore Sun (Nov. 30, 2020, 8:33 PM), https://www.baltimoresun.com/maryland/baltimore-county/bs-md-co-what-to-know-schools-ransomware-attack-20201130-2j3ws6yffzcrrkfzzf3m43zxma-story.html.

[180] Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 13 (2021), https://www.gao.gov/products/gao-20-644.

[181] *Id.*

[182] Federal Trade Commission, Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act 3 (2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online.

[183] *See* Center for Democracy & Technology, *Comments on California Privacy Protection Agency's Proposed Rulemaking Under the California Privacy Rights Act of 2020*, at 12-14, Nov. 8, 2021, https://cdt.org/wp-content/uploads/2021/11/CDT-Comments-to-Cal-Privacy-Protection-Agency-on-CPRA-Rulemaking.pdf (explaining the importance of scoping rules to protect student privacy without creating unintended consequences for service provision).

broadly applicable data-related rule may not apply as easily to entities providing government services and may even interfere with those services.[184]

iv. ID verification for government services

(Questions 2, 2a, 2b, 2c, 3, 3a, and 3b)

Both recipients of government services and victims of identity theft face risks from the use of private vendors by state and federal agencies providing benefits and services.[185] However, regulation of private vendors assisting with government service delivery presents a further challenge: just as with private providers of educational services, improperly considered rules may hamper the ability of government agencies to effectively deliver essential services. On the other hand, rules are clearly needed: the use and collection of citizen data by private companies poses risks to privacy that could result in material harm, such as identity theft; and government outsourcing of key benefits determinations to private companies can result in preventing some individuals from getting essential benefits.

The starting point for delivery of governmental services is identity verification, where the government agency checks that an applicant is who they say they are. As public agencies seek to modernize identity verification through data and technology use, they are increasingly considering incorporating assistance from private companies. Examples of vendor assistance include: attribute validation, where the vendor confirms that the information provided by an applicant matches that in other identity databases (such as driver's license data, health records, or financial records); and biometric verification, where the vendor confirms through the use of physical or biological information that the applicant matches any submitted identity documents (1:1 matching) or other biometric information in the vendor's database (1:many matching).[186] Most recently, the use of facial recognition as a kind of biometric verification has garnered widespread scrutiny.[187]

---

[184] For an analysis of how rules affecting private companies should be scoped to avoid unintended consequences for government service providers, *see* Center for Democracy & Technology, *Comments on FTC's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security*, at 48-51, https://cdt.org/wp-content/uploads/2022/11/CDT-Comments-to-FTC-on-ANPR-R111004.pdf.

[185] Here, we focus on practices that involve passing data to private technology vendors and exclude services that are provided solely by governmental entities or primarily involve in-person verification.

[186] *See* Michael Yang, Center for Democracy & Technology, *Digital Identity Verification: Best Practices for Public Agencies* (2022), https://cdt.org/insights/digital-identity-verification-best-practices-for-public-agencies/.

[187] Brian Naylor, *IRS Has Second Thoughts About Selfie Requirement*, NPR (Feb. 7, 2022, 3:29 PM), https://www.npr.org/2022/02/07/1078024597/want-information-from-the-irs-for-some-the-agency-wants-a-selfie.

The two main risks in the provision and use of such identification verification services are data breaches and biased algorithms.[188] First, when sensitive information is processed by a third party for purposes of identity verification, this data sharing increases the potential for data breaches. For example, ID.me, a facial recognition identity verification company, allowed employees to bring home devices that carried U.S. citizens' identity data and retained biometric data longer than necessary.[189] Such practices increase the chances of data being leaked onto the internet and later used for identity theft. Similar risks came to fruition when Equifax, a credit agency that also provides attribute validation for identity verification, exposed personal information of 147 million people in a 2017 data leak, allowing both domestic and foreign criminals to defraud state governments of pandemic unemployment assistance by using false or stolen identities.[190] Victims of identity theft face significant obstacles in re-asserting their identity and regaining access to government services.

Second, biometric analysis for identity verification may be less accurate for individuals from some racial backgrounds.[191] That bias harms members of those groups because they face increased barriers in accessing government services that require biometrics as part of identity verification. For this reason, the General Services Administration (GSA) committed in January 2022 not to use facial recognition, from private companies or otherwise, for identity verification in government service delivery until facial recognition is sufficiently free of biases.[192] However, the GSA's new rule is limited to the products that it deploys (namely, Login.gov, the single sign-on authentication solution it provides to other federal, state, and local agencies), and does

---

[188] Hannah Quay-de la Vallee, *Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives*, Center for Democracy & Technology (Jun. 7, 2022), https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/.

[189] Caroline Haskins, *Inside ID.me's Torrid Pandemic Growth Spurt, Which Led to Frantic Hiring, Ill-Equipped Staff, and Data-Security Lapses as Tte Company Closed Lucrative Deals With Unemployment Agencies and the IRS*, Bus. Insider (Jun. 7, 2022, 5:00 AM), https://www.businessinsider.com/id-me-customer-service-workers-hiring-secuirty-privacy-stress-data-2022-6. Jessy Edwards, *ID.me Lawsuit Claims Company Violates Data Storage Requirements*, Top Class Actions (Aug. 22, 2022), https://topclassactions.com/lawsuit-settlements/privacy/bipa/id-me-lawsuit-claims-company-violates-data-storage-requirements/.

[190] Cezary Podkul, *How Unemployment Insurance Fraud Exploded During the Pandemic*, ProPublica (July 26, 2021, 5:00 AM), https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.

[191] Nicol Turner Lee, *Mitigating Bias and Equity in Use of Facial Recognition Technology by the U.S. Customs and Border Protection*, Brookings Institution (July 27, 2022), https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/.

[192] *Executive Order 13985 – Equity Action Plan*, General Services Administration (Jan. 20, 2022), https://www.gsa.gov/cdnstatic/GSAEquityPlan_EO13985_2022.pdf.

not address bias in other forms of biometrics, like voice recognition.[193] Other government agencies at every level may still use biometrics from private vendors, regardless of levels of bias, for identity verification. Thus, other agencies should consider the appropriate level of accuracy and fairness for biometrics to be used safely, and establish that as the standard all private vendors must meet when providing biometric verification to government services on the ground.

v. Eligibility determination and allocation of benefits

(Question 2, 2a, 2b, 2c, 3, 3a, and 3b)

Government agencies also use private vendors' algorithm-driven systems to determine eligibility for, allocate, and verify legitimate provision of benefits. Private contractors develop many of these systems, some of which are off-the-shelf products while others are developed for specific populations in the jurisdictions where they are used. People with disabilities who are not able to work, or who can work only limited hours, may be reliant on public benefits – including Medicaid coverage for basic health care and long-term supports and services, housing assistance, food stamps, and cash assistance – that are subject to algorithm-driven decisions generated by private companies.

For instance, algorithmic systems are used in determinations about home- and community-based services to assess hours of care a beneficiary will need or the budget for providing necessary care.[194] Advocates have documented that in many cases, states' implementation of these systems has caused sudden, drastic, and arbitrary reductions or terminations of benefits that were previously granted. This has had devastating and terrifying effects on the lives of disabled and low-income people because it deprives recipients of care that supports independent living at home. Recipients cannot reasonably avoid such outcomes because reductions or terminations to their benefits often take effect before they are properly informed. For instance, one health services technology company, Optum, developed a needs assessment tool for Arkansas that cut approved care hours for some people with developmental disabilities in Arkansas nearly in half without explanation, putting them at imminent risk of serious injury and potential institutionalization, and preventing them from completing basic

[193] Claudia Lopez Lloreda, *Speech Recognition Tech Is Yet Another Example of Bias*, Scientific American (July 5, 2020), https://www.scientificamerican.com/article/speech-recognition-tech-is-yet-another-example-of-bias/.
[194] Lydia X.Z. Brown et al, Ctr. for Democracy & Tech., *Challenging the Use of Algorithm-Driven Decision-Making in Benefits Determinations Affecting People With Disabilities* (2020), https://cdt.org/insights/report-challenging-the-use-of-algorithm-driven-decision-making-in-benefits-determinations-affecting-people-with-disabilities/ [hereinafter *Benefits Determinations*].

daily functions like eating and using a bathroom.[195] Similarly, in Indiana, IBM's algorithm-driven system for processing welfare applications caused sudden termination of benefits for huge numbers of low-income people, who received confusing and delayed notices about noncompliance or fraud.[196]

While state agencies violate civil rights and constitutional protections when adopting systems that impose these harms, people currently have little to no recourse against the private companies that develop and sell these tools to arbitrarily and drastically cut people's benefits. Under Title II of the ADA, a person may not be excluded from participation in or denied benefits of the services of any "public entity" on the basis of disability.[197] Public benefits determinations that deprive recipients of benefits that allow them to live independently can force recipients to be institutionalized. This violates the ADA's community integration mandate that the Supreme Court affirmed in 1999, which requires government entities to administer government services and programs in a manner that enables disabled people to interact with non-disabled people in the most integrated setting possible.[198] Although government agencies should avoid procuring systems from private vendors that would interfere with disabled people's ability to continue living in their own homes, vendors are not precluded from selling tools that have this outcome.

Even when a benefits recipient is granted these services in the correct amount, the use of electronic visit verification (EVV) systems can interfere with the provision of personal care services. Similar to algorithmic systems used for benefits determination, EVV mobile apps and software are often provided by private home health tech companies.[199] With these systems, companies like Sandata and Direct Care Innovations require care workers to confirm that they are providing services as approved by interacting with facial recognition, voice verification, and

---

[195] *Id.* at 21. *See also* Upturn, Benefits Tech Advocacy Hub, *Arkansas Medicaid Home and Community Based Services Hours Cuts*, https://www.btah.org/case-study/arkansas-medicaid-home-and-community-based-services-hours-cuts.html; Ryan Calo & Danielle Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 Emory L.J. 797, 799 (2021), https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj.

[196] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, at 39-54 (2018); Rick Callahan & Tom Davies, *Judge: IBM Owes Indiana $78M for Failed Welfare Automation*, APNews (Aug. 7, 2017), https://apnews.com/article/8eb53eb9bdf94adb92e5b8b09559d8d0.

[197] 42. U.S.C. 12132.

[198] Brown, *Benefits Determinations*, *supra* note 194, at 17.

[199] Alexandra Mateescu, Data & Society, Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care 14 (2021), https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf. For a non-exhaustive list of private EVV vendors, *see* Applied Self-Direction, *Directory of EVV Vendors Interested in Serving Self-Direction Programs* (last updated Oct. 5, 2022), https://www.appliedselfdirection.com/resources/directory-evv-vendors-interested-serving-self-direction-programs.

GPS location tracking features during home visits.[200] Companies require workers to verify their service provision through their designated EVV systems frequently, with precision, and within narrow windows of time during their home visits to prove that benefits are not being abused.[201]

When a system incorrectly flags that workers did not provide services at the approved time and location, this delays payments until this flag is resolved, costing workers their wages.[202] This can also obligate recipients to pay for workers' lost wages out of pocket and to stay within the confines of their homes due to geofencing limits that cause their care workers to be flagged for fraud, and it reduces the home care workforce.[203] One company, CareBridge, plans to combine EVV technology with a predictive model to assess care needs, creating new risks for unreliable data practices to undercut provision of care.[204] This interferes with the care disabled people are supposed to receive as well as the wages that care workers (who are disproportionately women of color, and often disabled and from immigrant communities) can lose over minor errors or delays.[205]

E. Dark patterns

(Question 2)

---

[200] Sandata, *Ensure EVV Compliance with Multiple Verification Methods*, https://www.sandata.com/multiple-verification-methods-help-ensure-evv-compliance/; Direct Care Innovations, *High Tech and Low Tech Options for EVV* (Mar. 24, 2019), https://www.dcisoftware.com/blog/dci-evv-options/.
[201] Mateescu, *supra* note 199, at 30. *See also* Public Partnerships, *Time4Care Electronic Visit Verification (EVV) Mobile App*, https://www.publicpartnerships.com/tools/time4care-evv/.
[202] Virginia Eubanks & Alexandra Mateescu, *'We Don't Deserve This': New App Places US Caregivers Under Digital Surveillance*, The Guardian (July 28, 2021, 6:00 AM), https://www.theguardian.com/us-news/2021/jul/28/digital-surveillance-caregivers-artificial-intelligence; Jacqueline Miller et al., University of California San Francisco Health Workforce Research Center on Long-Term Care, *Impact of Electronic Visit Verification (EVV) on Personal Care Services Workers and Consumers in the United States* 12, 15-16 (2021), https://healthworkforce.ucsf.edu/sites/healthworkforce.ucsf.edu/files/EVV_Report_210722.pdf.
[203] Eubanks, *supra* note 202; Naomi Gallopyn & Liza I. Iezzoni, *Views of Electronic Visit Verification (EVV) Among Home-Based Personal Assistance Services Consumers and Workers*, Disability and Health Journal (2020), https://www.ancor.org/wp-content/uploads/2022/08/disability_and_health_journal_article_on_views_of_evv.pdf.
[204] *CareBridge Launches to Improve Care for Individuals Receiving Long-Term Support Services*, Business Wire (Jan. 12, 2020, 4:58 PM), https://www.businesswire.com/news/home/20200113005935/en/CareBridge-Launches-Improve-Care-Individuals-Receiving-Long-Term.
[205] Id at 45-46. See also Lydia X.Z. Brown, *EVV Threatens Disabled People's Privacy and Dignity – Whether We Need Care, or Work as Professional Caregivers*, Ctr. for Democracy & Tech (Mar. 24, 2022), https://cdt.org/insights/evv-threatens-disabled-peoples-privacy-and-dignity-whether-we-need-care-or-work-as-professional-caregivers/.

Dark patterns include misrepresentations of how account holders' selected privacy settings are implemented,[206] and misrepresentations that trick or trap people into providing consent.[207] Certain practices involve deploying user interface and design elements that people would be expected to overlook, misunderstand, or be manipulated by, inducing people to provide data or agree to certain uses of their data when they may not otherwise.[208] As a result, dark patterns deny people the ability to navigate websites and apps freely by making them responsible for avoiding manipulative elements they may not even recognize.[209]

Dark patterns come in a variety of options. One prominent type of dark pattern is hidden information, where a company provides people's options or the information needed to compare those options in fine print text or in faded text.[210] In the same situation, misdirection, or aesthetic manipulation, can be used to distract people to pay attention to the company's preferred options, for example by providing their preferred options or information about those options in contrasting, more eye-catching colors.[211] This is further exacerbated by preselection, another type of dark pattern where a choice is already selected by default – for instance, an already checked box indicating acceptance of terms of service or opt-in to a mailing list – which increases the likelihood that people will proceed with the selected option instead of looking at others.[212] There are several other dark pattern types as well,[213] including situations in which

---

[206] Federal Trade Commission, *Facebook Settles FTC Charges That it Deceived People by Failing to Keep Privacy Promises* (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-people-failing-keep-privacy-promises.

[207] Federal Trade Commission, *Children's Online Learning Program ABCmouse to Pay $10 Million to Settle FTC Charges of Illegal Marketing and Billing Practices* (Sept. 2, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing.

[208] *See generally* Jamie Luguiri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Legal Analysis 43 (2021), https://academic.oup.com/jla/article/13/1/43/6180579; Alfred Ng & Sam Morris, *Dark Patterns That Mislead Are All Over the Internet*, The Markup (June 3, 2021, 10:00 AM), https://themarkup.org/2021/06/03/dark-patterns-that-mislead-people-are-all-over-the-internet.

[209] Lauren E. Willis, *Deception by Design*, 34 Harvard J. L. Tech. 133-34 (2020), https://jolt.law.harvard.edu/assets/articlePDFs/v34/3.-Willis-Images-In-Color.pdf; Federal Trade Commission, *Bringing Dark Patterns to Light* 23-27 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

[210] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, & Austin L. Toombs, *The Dark (Patterns) Side of UX Design*, 7 (2018) https://dl.acm.org/doi/pdf/10.1145/3173574.3174108.

[211] *Id.*; Luguiri, *supra* note 208, at 51; Deceptive Design, *Misdirection*, https://www.deceptive.design/types/misdirection.

[212] *Id.*

[213] Deceptive Design, *Types of Deceptive Design*, https://www.deceptive.design/types.

privacy-invasive defaults are in place and privacy settings are intentionally made difficult for people to navigate, likely leaving these defaults in place.[214]

Dark patterns can affect people differently depending on the devices they are using and barriers they may experience with respect to digital literacy. User experiences with dark patterns can differ between mobile and web modalities, so a company might use dark patterns only in one modality, treating people differently according to the devices on which they are accessing the company's service.[215] Therefore, the company's potential uses of dark patterns would need to be scrutinized across all modalities through which it provides the service. Further, on top of the information asymmetry that people in general face when it comes to data collection and processing, education level is shown to affect susceptibility to more subtle dark patterns, indicating that communities with inequitable access to education may be more likely to be manipulated.[216] With the emergence of new media types such as augmented and virtual reality, dark patterns may become even more difficult for people to recognize.[217]

II. How regulators, legislators, and stakeholders should approach implications of harmful data practices

(Question 1, 1a, and 3f)

A. "Privacy" as the framework for discussing civil rights and equity implications

(Question 1a)

Policymakers and stakeholders must recognize that protecting privacy is integral to protecting civil rights, and vice versa. When people's data is overcollected, when it is used for secondary purposes without consent or otherwise inappropriately repurposed, or when it is processed to affect access to fundamental life opportunities, this exploitation of data creates heightened harms for marginalized groups. When algorithm-driven systems or features are used for facially neutral purposes but treat certain marginalized groups differently, they can violate these groups' privacy by collecting and processing data that may be unnecessary and unrelated to the

[214] Deceptive Design, *Privacy Zuckering*, https://www.deceptive.design/types/privacy-zuckering; Luisa Jarovsky, *Dark Patterns in Personal Data Collection: Definition, Taxonomy, and Lawfulness* 30-31 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4048582.
[215] *See* Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, & Christo Wilson, *A Comparative Study of Dark Patterns Across Mobile and Web Modalities*, 5 Proceedings of the ACM on Human-Computer Interaction 22 (2022), https://cbw.sh/static/pdf/gunawan-2021-pacmhci.pdf.
[216] *See* Luguiri, *supra* note 208, at 70-71.
[217] *See* Michal Turjeman, *Designing the Metaverse: Challenges and Questions*, VentureBeat (July 24, 2022, 1:10 PM), https://venturebeat.com/datadecisionmakers/designing-the-metaverse-challenges-and-questions/.

purported purpose. Therefore, all consumers should be protected from data abuses and empowered to access information, opportunities, and services online without risks of discrimination or inequitable outcomes.[218]

B. Impact of consolidation in tech and telecom

(Question 3f)

While there are some smaller privacy-protective companies, most large tech companies, including the most prominent social media companies, overcollect data. People cannot avoid this overcollection by moving to competing services because few exist. Those competitors that do exist suffer from lack of network effects, making them undesirable for most people to join. For example, it is likely impossible for most people to recreate their Instagram networks on BeReal. Therefore, providing choices to users through competition is one important spur for companies to innovate and provide better quality products and services, including better privacy protections. Nevertheless, companies are incentivized to collect more and more data about a person and their activities, interests and vulnerabilities. This incentive for collection of data leads to a variety of harms to people resulting from practices, including, as noted above: unwanted data collection and retention; unwanted and unexpected secondary use of data; unwanted combination of data across contexts; and unwanted disclosure of personal information to advertisers or to others. The current advertising ecosystem provides a key example of these harms.

i. Role of competition in advertising

The opaque system of online behavioral advertising has provided an incentive for over-collection and retention of data by a broad range of parties. Consumer Reports has cataloged the extensive tracking of online activities throughout people's day-to-day lives by several major technology platforms, often incentivized or practiced by ad tech companies.[219]

---

[218] *Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security, Hearing Before the H. Comm. on Energy and Commerce, Subcomm. On Consumer Protection and Commerce*, 117th Cong., June 14, 2022 (testimony of David Brody, Managing Attorney, Digital Justice Initiative, Lawyers' Committee for Civil Rights Under Law).

[219] Justin Brookman, *Understanding the Scope of Data Collection by Major Technology Platforms*, Consumer Reports (May 2020), https://digital-lab.consumerreports.org/wp-content/uploads/2021/02/Understanding-the-scope-of-data-collection-by-major-platforms_2020_FINAL.pdf.

With other civil rights and consumer protection organizations, we previously identified dozens of different kinds of harm from commercial data practices, particularly invasions of privacy.[220]

Importantly, data overcollection for behavioral advertising is practiced not just through websites and smartphone apps, but through other parties as well. For example, Internet Service Providers have been found to collect data that is unnecessary for the provision of Internet service, share that data with third parties, and use that data to target advertising.[221] Surveillance by a network provider is especially opaque: the user may not know or intentionally interact with a network provider (for example, at your workplace, school or a friend's home) and typically does not directly use a piece of software with a clear user interface or privacy information. Furthermore, the network provider has access to all traffic, even if the consumer switches to a different app, or uses another device altogether. And network providers have access to consumer data that may frustrate attempts to use technical precautions to protect privacy. For example, encrypting network traffic may help users, but a network provider can still learn about online activity through traffic analysis. Turning off location services in your smartphone's operating system will not prevent cellular carriers from learning your location when you make and receive calls. And network providers can collude with online trackers to undermine the ability to clear cookies or reset data from one's own device.[222] Ubiquitous online behavioral advertising without user understanding or control has provided an incentive for this class of businesses not just to provide the Internet access that a consumer believes they're purchasing, but also to start additional businesses in ad targeting, or to sell data to third parties.

Behavioral advertising contributes not just to the incentive for overcollection, but also to the broad dispersion and disclosure of data, including sensitive information, in an unregulated ecosystem. As noted above, consider the example of location information accessible by mobile apps, including dating apps. Location might be useful for finding nearby matches and people to talk to. But the incentive to sell data for behavioral advertising has led in some cases to sale of that location data for ad targeting and to data brokers, and in one notable case the disclosure of someone's sexual orientation and activity. This was not limited to a single transaction between

---

[220] Letter from Civil Society Organizations to FTC Chair Lina Khan and FTC Commissioners, (Aug. 4, 2021), https://cdt.org/wp-content/uploads/2021/08/2021-08-04-FTC-civil-rights-and-privacy-letter-Final.pdf

[221] Federal Trade Commission, *A Look at What ISPs Know About You: Examining Privacy Practices of Six Major Internet Service Providers* (2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[222] In 2017, the FTC approved a settlement with Turn, an ad targeting firm, for working with cellular carrier Verizon Wireless to track online activity even after the user had specifically cleared cookies.

an app and an ad network. Instead, detailed location information was distributed through the real-time bidding process that allows advertisers to bid on placements of ads to people based on that behavioral data. As a result, one spokesman for a broker of consumer data concluded that "every single entity in the advertising ecosystem has access to the information shared by Grindr and every other app that uses the real-time bidding system. That means thousands of entities have such access."[223]

Online publishers currently often lack transparency and trust in the online advertising that they rely on for funding, and cross-context behavioral targeting lets online advertisers use detailed information gleaned from surveillance of a user on high-quality context-rich sites to advertise in other contexts, drawing money away from those publishers who might otherwise benefit from providing high-value contextual advertising. The model of building behavioral profiles that combine data across all online and offline activities creates incentives towards consolidation, and consolidation of the advertising market has inhibited competition. Publishers and content creators who rely on online advertising for funding pay what is in effect a heavy tax, to the dominant advertising technology firms and to a variety of vendors needed to mitigate losses within an untrusted ecosystem. Moves toward innovative models that would let people actively and voluntarily participate in customizing and selecting relevant online advertising have been undermined by advertising services that see no need to provide meaningful transparency or effective controls.

ii. Promising incentives for competition

There are some signs of competitive market incentives already at work. In response to growing consumer awareness, some online companies are strengthening their commitment to protecting personal data, including:

- investing additional resources in data security infrastructure;
- limiting their own retention and use of personal data;
- developing technologies to minimize the data collected to provide new services;
- providing tools to protect against commercial surveillance;
- encrypting more communications to protect personal data from hackers and foreign governments;
- enabling simpler and more understandable consumer choices;

[223] Byron Tau & Georgia Wells, *Grindr User Data Was Sold Through Ad Networks*, Wall St. J. (May 2, 2022), https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800.

- making commercial data practices more transparent and easier to understand.

These market-driven motivations should be enabled and encouraged.

III. Guiding principles and actions for Administration

A. Data minimization, use and purpose limitations, retention, deletion

(Question 5d)

The responsibility for preventing data misuse should not be left to the people affected by it. In many cases, the responsibility for keeping people's data private properly belongs with the entities collecting and using the data, rather than with individual people. There should be meaningful limits on how companies handle data in the first place to address harms that are cross-cutting, sector-specific, and specific to particular classes of underserved people.[224] Data collection, retention, processing, and sharing should be restricted to only as much as is necessary to fulfill the purpose for which people are choosing to engage with the company that deploys the data practices in question.[225] If companies need such data to provide their service to their customers, then collection should be allowed. But companies should not be allowed to collect any data they want in the hopes that they can monetize it through advertising or sale, or otherwise use it for purposes unrelated to the service.

Appropriate data minimization requirements for sensitive data would restrict:

- The collection of sensitive data to only data that is strictly necessary to provide the service requested by the consumer.[226]
- Secondary uses or repurposing of sensitive data.[227]

---

[224] *See generally* Consumer Reports & Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

[225] *See* Pre-rulemaking Stakeholder Session before the Cal. Privacy Protection Agency (2022) (testimony of Eric Null, Director of Privacy & Data Project, Center for Democracy & Technology), https://cdt.org/wp-content/uploads/2022/05/CA-Testimony-Eric-Null-Data-Minimization-Letterhead.pdf.

[226] Ideally the definition of "sensitive data" would be broad and expandable.

[227] *See* Pre-rulemaking Stakeholder Session before the Cal. Privacy Protection Agency (2022), (testimony of Andrew Crawford, Senior Policy Counsel, Center for Democracy & Technology) https://cdt.org/wp-content/uploads/2022/05/Andrew-Crawford-5-6-22-CPPA-Statement.pdf; Andrew Crawford & Michelle Richardson, *CDT & EHI's Proposed Consumer Privacy Framework for Health Data* 15, 23-27, Center for Democracy & Technology (2021), https://cdt.org/insights/cdt-ehis-proposed-consumer-privacy-framework-for-health-data/.

- The retention of sensitive data after the purpose for which the data was collected, used, and stored has been fulfilled.
- Any use, processing, or sharing of sensitive data after it has been shown to pose unmitigated risks to people.
- The use of people's sensitive data to target advertisements.[228]
- The use of settings or interfaces or other representations that are likely to mislead people as to how their personal data is handled, or to induce people's disclosure of data, so as to affect reasonable people's conduct with respect to the product or service.[229]

While properly de-identified data can be used in privacy-protecting ways, de-identified and aggregated data sets should not be viewed as absolute privacy protections – they can often be reidentified.[230] Even when appropriate steps are taken to protect individual privacy, people can still be re-identified and harms can still result. Aggregated and de-identified data sets can still mischaracterize underrepresented groups and thus result in disparate impacts. Therefore, other measures such as selective redaction of sensitive data from amassed data should also be incorporated.[231]

These considerations would help reduce harms arising from certain uses or categories of data that present heightened risks, and existing work can help shape how these considerations are approached when protecting sensitive data. For example, to address health data that falls outside of HIPAA and its associated Privacy Rule, policymakers should look to the AMA's Privacy Principles,[232] and consider the protections contemplated and outlined in the CDT/EHI Proposed

---

[228] There may be some limited instances where this is allowed, like if a consumer specifically opts into behaviorally targeted advertising.

[229] *See* Center for Democracy & Technology, *CDT's Federal Baseline Privacy Legislation Discussion Draft* 9 (2018), https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.

[230] *See e.g.,* Thompson, *supra* note 64. European researchers "have published a method they say is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes." Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data,* TechCrunch (Jul 24, 2019, 6:30 AM), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/; Justin Sherman explains how "[r]eidentification has become horrifyingly easy." Justin Sherman, *Big Data Might Not Know Your Name. But It Knows Everything Else,* Wired (Dec. 19, 2021, 8:00 AM), https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/.

[231] Nick Doty, *Selectively Redacting Sensitive Places from Location Data to Protect Reproductive Health Privacy*, Center for Democracy & Technology (Aug. 25, 2022), https://cdt.org/insights/selectively-redacting-sensitive-places-from-location-data-to-protect-reproductive-health-privacy/.

[232] American Medical Association, *AMA Privacy Principles* (2020), https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf.

Consumer Privacy Framework for Health Data[233] along with CDT's associated report.[234] These considerations include:

- Moving beyond outdated privacy models that place too much emphasis on notice and consent, which put unreasonable burdens on people to read and understand each company's voluminous and dense privacy policies, and that fail to articulate data use limits;
- Covering all information that can be used to make inferences or judgments about, or otherwise misuse, a person's sensitive characteristics; and
- Covering all entities that collect, disclose, or use consumer sensitive information, regardless of the size or business model of the covered entity.

Note that not all sensitive data uses, including those that utilize health and location data, are harmful. There are examples where health and location data can be utilized in a manner that both recognizes and protects individual user privacy, while also offering insights that can benefit public health and allow for dramatic improvements in health outcomes.[235] However, as detailed in Part I, current laws and regulations do not prevent harmful uses, so new efforts must be rooted in fair and equitable principles and balance the benefits to people with risks.

Appropriate requirements would restrict data brokers from:

- Sharing or selling to third parties any data of people whose consent is not meaningfully informed and freely given in a way that specifies the context and scope for which they consent.
- Failing to provide effective opt-out mechanisms such as those discussed in Section II.
- Repurposing consumer data provided to another entity in ways that are inconsistent with people's reasonable expectations of the entity to whom the data was originally provided.[236]
- Misrepresenting the network of third parties with whom data will be shared.

---

[233] The privacy principles embodied in the framework are not limited to only apply to self-regulatory regimes. Indeed, the principles were drafted to help both the public and private sectors better protect the privacy of people's health data. Crawford & Richardson, *supra* note 227.

[234] Crawford, *Placing Equity*, *supra* note 44.

[235] *See e.g.,* Mana Azarmi & Andrew Crawford, Center for Democracy & Technology, *Use of Aggregated Location Information and COVID-19: What We've Learned, Cautions about Data Use, and Guidance for Companies* 5-6 (2020), https://cdt.org/wp-content/uploads/2020/05/2020-05-29-Use-of-Aggregated-Location-Information-and-Covid-19.pdf.

[236] *See* Testimony of Andrew Crawford, *supra* note 227; Crawford & Richardson, *supra* note 227.

Appropriate data minimization requirements for discriminatory data-driven decision-making would prohibit:

- The use of decision-making systems that evaluate data related to protected characteristics, or are heavily influenced by data that tend to disproportionately disadvantage marginalized communities, when
    - The data is unrelated to people's ability to fulfill the obligations they would incur if approved for the prospective opportunity, or
    - There are effective, less discriminatory alternatives to such decision-making systems.
- Continued use or analysis of consumer data through a method that has been shown to disproportionately harm marginalized people.

B. Easily accessible privacy controls

(Question 1b)

People want their sensitive data protected and kept private. For example, when it comes to data about people's health, a recent American Medical Association (AMA) survey of patients found that they "are deeply concerned over the lack of security and confidentiality of personal health information."[237] The survey found that more "than 92% of people believe privacy is a right and their health data should not be available for purchase by corporations or other individuals."[238] Regarding financial information, in a 2021 Financial Health Network survey of over 2,000 people, respondents overwhelmingly preferred limits to data collection and sharing and greater control: 94% prefer that financial institutions do not share their data for marketing purposes, and 87% want to minimize fintech platforms' data collection to only the data needed.[239] In addition, 89% of people prefer that financial institutions' and fintech platforms' data sharing be subject to people's express opt-in, and 93% do not want fintech platforms to share their data with third parties for marketing purposes.

---

[237] American Medical Association, *Patient Perspectives Around Data Privacy* (2022), https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf.

[238] *Id.* The Survey also found the following:

• Almost 80% of participants want to be able to "opt-out" of sharing some or all their health data.

• More than 75% of patients want to opt-in before a company uses any of their health data.

• More than 75% of people want to receive requests prior to a company using their health data for a new purpose.

[239] Dan Murphy, David Silberman, & Stephen Arves, Financial Health Network, *Financial Data: The Consumer Perspective* 9-15 (2021), https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf.

Meaningful, direct limitations and data minimization requirements put the least burden on people. But effective consumer controls can be an additional complement, allowing people to select the data use practices that work for them. For control requirements to be effective, controls must be, wherever feasible, universal preferences. Forcing people to opt out of data collection, sharing or re-use on every interaction in an online environment with widespread commercial surveillance is unreasonably burdensome, and would be equivalent to no genuine controls at all.

Opt-out control mechanisms should also be standardized to ease adoption by industry and to facilitate effective choices by people, in a way that respects existing opt-out and consumer preference mechanisms, including the Global Privacy Control.[240] Clear regulatory guidance and enforcement of expressed preferences have been identified as needs for the successful standardization and widespread adoption of this class of consumer-controlled preference mechanism.[241]

Additional privacy-preserving advertising techniques are also possible, and could see further investment in response to signals from new regulatory requirements to provide people with more effective controls and context-based limits on the use of their personal information. Proposals deployed by browser vendors or proposed in technical standard-setting bodies include on-device auctions based on selected audiences or cohorts of interest topics. To the extent that many people see a benefit in personally targeted advertising, there are alternative techniques that can provide greater control, satisfaction, and data quality from people who choose to opt in and list their specific interests. The greatest impediment to progress on any of this class of proposals today is the lack of uptake from advertising firms who rely on and benefit from a status quo where people can be ubiquitously tracked and targeted with little transparency or effective control. Absent effective rules that promote consumer-controlled advertising, we do not expect the requisite work on development and adoption of these alternative advertising practices.

Some companies will turn to practices that specifically undermine user control and consumer privacy once rules are in place and once increased technical mitigations are deployed. Privacy protections developed by online platforms – including web browsers and mobile operating

[240] Global Privacy Control, https://globalprivacycontrol.org/. *See also* Cal. Civ. Code §1798.135(a)-(b); Colo. Rev. Stat §6-1-1313.
[241] Nick Doty, *Enacting Privacy in Internet Standards* 74-75 (University of California, Berkeley 2020), https://npdoty.name/writing/enacting-privacy/drafts/enacting-privacy-20201219.pdf.

systems – have led to similar kinds of industry workarounds that can maintain pervasive cross-context tracking of user behavior while circumventing user controls. Browser or device fingerprinting is one notable example, where a website or app will collect many different observable characteristics about the configuration of a device or browser to create a unique fingerprint that can track activity across multiple contexts without the user's knowledge or consent.[242] But there are many additional novel tracking techniques, including bounce tracking, and, more recently, direct solicitation of personally identifiable information that can be used for the secondary purpose of combining the user's data across many different contexts.

The technical community has recognized that for some technical circumventions of privacy protections, technical protections will likely always be incomplete or insufficient, and that there is a specific need for regulation, investigation, and enforcement from authorities to both protect privacy and provide a level playing field to companies that do not circumvent people's choices.[243]

C. Third-party audits and transparency

(Questions 6b, 6c, and 6e)

Reliance on industry codes of conduct or self-certification standards might enable companies to narrow their disclosures so that they can technically comply without offering true transparency.[244] Instead, both industry and policymakers could look to resources such as the *Civil Rights Standards for 21st Century Employment Selection Procedures* for guidance on more reliable and robust auditing and transparency measures that would ensure fairer and more equitable decision-making processes and that would be scoped to the information needs of affected people and regulators.[245] While this resource focuses on employment, it offers detailed recommendations that could be adapted broadly, including:

---

[242] *See* Peter Eckersley, Electronic Frontier Found., *How Unique Is Your Web Browser?*, Proceedings of the 10th Int'l Symp. on Privacy Enhancing Technologies 4 (2010), https://coveryourtracks.eff.org/static/browser-uniqueness.pdf.

[243] *See e.g.,* World Wide Web Consortium (W3C) Technical Architecture Group, *Unsanctioned Web Tracking* (2015) https://www.w3.org/2001/tag/doc/unsanctioned-tracking/.

[244] Inioluwa Deborah Raji, I. Elizabeth Kumar, Aaron Horowitz, and Andrew D. Selbst, *The Fallacy of AI Functionality*, Proceedings of the 2022 ACM Conf. on Fairness, Accountability & Transparency 959, 966, https://dl.acm.org/doi/pdf/10.1145/3531146.3533158.

[245] In 2022, CDT published the *Civil Rights Standards for 21st Century Employment Selection Procedures* in partnership with the ACLU, the American Association for People with Disabilities, the Leadership Conference on Civil and Human Rights, the National Women's Law Center, and Upturn. The *Civil Rights Standards* offer guidance for employers, vendors, and policymakers, but they can be adapted for other specific contexts and for broader application. *Civil Rights Standards for 21st Century Employment Selection Procedures* (2022), https://cdt.org/insights/civil-rights-standards-for-21st-century-employment-selection-procedures/.

- Multiple tiers of notice to ensure that affected people understand how an automated system may affect them, and that regulators can examine whether the system is subject to their enforcement authority;
- Pre-deployment auditing steps that would examine an automated system's potential discrimination risks before it can impact anyone;
- Ongoing auditing that enables companies and other users of automated systems to recognize and address previously undetected risks.

At minimum, effective transparency measures would (subject to any applicable First Amendment limits):

- Require companies to perform algorithmic impact assessments that proactively examine the practice's fitness for purpose, potential risks of disparate impact affecting all marginalized identities that may be subjected to the practice, and mitigating measures, and making assessment results or their summaries publicly available. Companies should not be permitted to use, sell, or provide a technology, online platform, or software that they claim to be nondiscriminatory if they do not provide pertinent information about the tool's impacts on all marginalized identities that may be subject to the tool, or if they obligate consumers to provide personal data to access the results or summaries of impact assessments.
- Establish that the information companies must disclose about their data practices should be provided in two forms: a shorter, easy-to-understand form with enough detail to enable consumers to interact with companies' platforms without being harmed, and a more thorough form with enough detail to enable regulators' enforcement. Companies must provide meaningful information to consumers before and after collecting, processing, or sharing consumer data, explaining the purpose for which the practice is used, reasons for possible and actual adverse decisions, factors that contribute to such decisions, and people's available alternatives to the data practice.
- Require disclosures to be available in multiple commonly spoken languages and in plain language to ensure that all consumers are actually informed about how their data is handled. Companies must recognize that non-English-speaking consumers, consumers with disabilities – including blindness and disabilities affecting cognitive processing – and communities who experience barriers to education are entitled to this information.
- Enable comparison and easy understanding through standardized, short-form notice that is relevant to the context and medium. In other sectoral privacy laws and in other areas

where consumers are expected to quickly comprehend product information,[246] standardized labels have been successful in enabling consumers to compare and make informed choices.

Question 5a asks whether these principles are reflected in any legislative proposals. Many of the principles discussed in Part III(A)-(C) are reflected in the bipartisan American Data Privacy and Protection Act (ADPPA), which the House Energy & Commerce Committee introduced and passed out of committee in 2022. The ADPPA would apply the data minimization, opt-out, and transparency requirement identified above, in addition to civil rights protections for data practices.[247] In response to questions 5b and 5c, the ADPPA's protections would raise the bar for all Americans, preventing privacy harms regardless of age. Layered on top of that are additional protections for children, primarily a ban on targeted advertising and an opt-in consent requirement for transfer of children's data.[248] Further, the ADPPA was drafted to recognize the need to treat government service providers differently from other private companies, so as to not impede the administration of government services. Amendments to the ADPPA ensured that governmental entities are not "covered entities" under the bill and that their contractors would be treated as "service providers" who are not directly subject to the bill's requirements for "covered entities."[249]

---

[246] *See e.g.*, 15 U.S.C. §6801 et seq; Lorrie Faith Cranor, Pedro Giovanni Leon, & Blase Ur, *A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices*, 10 ACM Transactions on the Web, no. 3 (Aug. 26, 2016): 17:1-17:33. https://doi.org/10.1145/2911988; Brian X. Chen, *What We Learned From Apple's New Privacy Labels*, N.Y. Times (Jan. 27, 2021), https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html; Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, *in* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1573–82 (2010), https://doi.org/10.1145/1753326.1753561. Note that research has also shown challenges with comprehensibility of existing labels and recommended improvements. *See* Yucheng Li, Deyuan Chen, Tianshi Li, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong, *Understanding IOS Privacy Nutrition Labels: An Exploratory Large-Scale Analysis of App Store Data*, *in* Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems, 1–7 (2022), https://doi.org/10.1145/3491101.3519739.

[247] Eric Null, *On This Year's International Data Privacy Day, Let's Keep Pushing for National Privacy Protections*, Center for Democracy & Technology (Jan. 26, 2023), https://cdt.org/insights/on-this-years-international-data-privacy-day-lets-keep-pushing-for-national-privacy-protections/.

[248] Center for Democracy & Technology, *CDT Letter to House Energy & Commerce Staff on Bipartisan Privacy Bill, American Data Privacy and Protection Act* (June 13, 2022), https://cdt.org/insights/cdt-letter-to-house-energy-commerce-staff-on-their-bipartisan-privacy-bill/.

[249] H.R. 8152, Amendment in the Nature of a Substitute #1 (H8152_ANS_FC_02) sec. 2(9)(B)(i)-(ii), (29)(A)(ii), 117th Cong. (2002), https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115041 (including entities that provide services to governmental entities as "service providers" but excluding them from the scope of "covered entities").

D. Other actions the federal government can take

(Question 5e and 6a)

Where the use of data and technology discriminates against legally protected classes, agencies should coordinate to make full use of their enforcement authorities. Coordination could identify which agencies would address which harms, based on their respective experience, resources, and enforcement priorities, as well as conducting joint investigations. Such coordination could be memorialized in a memorandum of understanding or other documentation. The recent Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government specifically describes the need for cross-agency coordination to ensure that equity and civil rights enforcement are built into agencies' use and regulation of technology.[250] This will require modernized guidelines from federal agencies with authorities to enforce civil rights laws to facilitate enforcement against data-driven discrimination and inequity. It will also require agencies like the FTC and CFPB to use their authorities under consumer protection laws such as the FTC Act, the FCRA, and the Consumer Financial Protection Act to enforce against unfair or deceptive data practices, inappropriate data sharing, and inaccurate data reporting to prevent discriminatory or inequitable outcomes.[251]

As the RFC notes, to ensure that agencies use their authorities in alignment with the best interests of people most affected by data practices, agencies must solicit input from marginalized groups. Meaningful public engagement will require agencies to provide notice about policymaking activities and conduct public hearings in ways that maximize public participation, including with language access and disability access. This includes providing plain-language notices and explainers regarding policymaking activities, ASL interpretation and captioning services for hearings, virtual and in-person options to participate in hearings, and post-hearing transcripts.

---

[250] Executive Order 14091, *Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, Feb. 16, 2023.

[251] See e.g., Dell Cameron, *How the US Can Stop Data Brokers' Worst Practices – Right Now*, Wired (Feb. 8, 2023, 7:00 AM), https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/; Eric Null & Nathalie Maréchal, *CDT Joins Coalition in Urging CFPB to Protect Consumers' Financial Privacy*, Center for Democracy & Technology (Feb. 8, 2023), https://cdt.org/insights/cdt-joins-coalition-in-urging-cfpb-to-protect-consumers-financial-privacy/; Center for Democracy & Technology, *Comments on FTC's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security*, Nov. 21, 2022, https://cdt.org/insights/cdt-comments-to-ftc-regarding-prevalent-commercial-surveillance-practices-that-harm-consumers/.

IV. Conclusion

The RFC illustrates the NTIA's deep engagement with a diverse array of public stakeholders, recognizing the communities that must be protected from data-driven harms under existing civil rights and privacy laws as well as communities who are marginalized but remain unprotected under any existing frameworks. CDT looks forward to supporting the NTIA's ongoing efforts to guide the federal government toward ensuring that privacy, equity, and civil rights are prioritized in new policymaking.