LAWYERS' COMMITTEE FOR
CIVIL RIGHTS
UNDER LAW

STATEMENT OF DAVID BRODY

MANAGING ATTORNEY OF THE DIGITAL JUSTICE INITIATIVE

LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW

U.S. HOUSE COMMITTEE ON ENERGY AND COMMERCE

INNOVATION, DATA, AND COMMERCE SUBCOMMITTEE

HEARING ON

LEGISLATIVE SOLUTIONS TO PROTECT KIDS ONLINE AND ENSURE AMERICANS' DATA PRIVACY RIGHTS

APRIL 17, 2024

I. Introduction

Chair Bilirakis, Ranking Member Schakowsky, and Members of the Subcommittee, thank you for the opportunity to testify today on bipartisan, bicameral legislation that seeks to strengthen data privacy, security, and civil rights. My name is David Brody, and I am the Managing Attorney of the Digital Justice Initiative at the Lawyers' Committee for Civil Rights Under Law ("Lawyers' Committee").

The Lawyers' Committee uses legal advocacy to achieve racial justice, fighting inside and outside the courts to ensure that Black people and other people of color have voice, opportunity, and power to make the promises of our democracy real. The Lawyers' Committee works at the intersection of racial justice, technology, and privacy to address predatory commercial data practices, discriminatory algorithms, invasions of privacy, disinformation, and online harms that disproportionately affect Black people and other people of color, including people with intersectional identities, like immigrants, women of color, and LGBTQI+ people of color.

We care about privacy because it ensures that who we are cannot be used against us unfairly. That is why privacy rights are civil rights. The "inviolability of privacy," the Supreme Court wrote in its landmark decision in *NAACP v. Alabama*, is "indispensable to preservation of freedom of association."[1]

But our nation **lacks** a strong federal privacy standard, so online, our identities and behaviors **are used against us**. Data about Black communities and other historically marginalized communities often reflects the history of inequality and segregation in this country. That data is collected by technology companies, fed into algorithms, and used to make decisions affecting the lives of the people in those communities. Too often this data is used to deny equal opportunities and freedoms. Attached to my testimony is a forty-three-page appendix documenting the extensive evidence of disparate harms and unequal access to goods and services that consumers of color continue to face due to discriminatory algorithms and exploitative data practices, complete with two-hundred and fifty-five footnotes of examples.

This dynamic is deeply contrary to cornerstone principles and promises of equal access and a level playing field for everyone. Without strong privacy and online civil rights protections, discrimination will continue to infect the digital marketplace.

That's why we are encouraged by the new American Privacy Rights Act (APRA), a bipartisan and bicameral effort to safeguard data privacy and civil rights online. Passing comprehensive privacy legislation would be a major advancement for the public good. I would like to thank Chair McMorris Rodgers and Senator Cantwell

[1] *NAACP v. Alabama*, 357 U.S. 449, 462 (1958).

for producing this impressive achievement. This bill represents significant progress since this committee last considered comprehensive privacy legislation two years ago, the American Data Privacy and Protection Act (ADPPA). The Lawyers' Committee looks forward to working with both chambers to strengthen the bill.

Like the American Data Privacy and Protection Act, the American Privacy Rights Act would effectively establish "building codes for the Internet." Just as construction regulations enable us to build safe homes and physically expand upwards and outwards, so too will strong data protection rules establish an infrastructure for American leadership in online commerce. These foundational rules include data minimization, civil rights and consumer protections, transparency, data security, individual rights to control one's data, and multilayered enforcement.

The American Privacy Rights Act, however, has several key improvements over previous legislation. It prohibits forced arbitration of claims involving discrimination or other "substantial privacy harms." It allows individuals to opt-out from algorithms that would make consequential decisions about them based on personal data. It has stronger protections for health data. The Act shortens the timespan individuals would have to wait before they can enforce their rights. And it prohibits "dark patterns" that impair and individual's control over their own data.

But the bar for comprehensive privacy legislation has also been raised in the last two years, as states have enacted more privacy and civil rights protections for their citizens. Many states are passing or considering comprehensive privacy laws. Some of these are fairly protective, such as California's and Maryland's, while many others are inadequate, such as Virginia's statute and its copycats.[2] Maryland recently passed legislation—modeled on this committee's past work—with strong civil rights protections and a mandate that companies only collect as much data as is necessary to provide a service requested by the consumer.[3] California has continued to strengthen its privacy laws by issuing new regulations, adding protections for data on mental health and sexuality, and passing new requirements for data brokers.[4] Washington state passed the My Health, My Data Act which strictly limits secondary use of personal health information.[5] Illinois leads the nation on biometric privacy protections.[6] Dozens of other innovative privacy proposals are advancing in state legislatures, including in Vermont, Maine, and Massachusetts.[7] States are also

[2] Caitriona Fitzgerald et al., *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, ELEC. PRIV. INFO. CTR. & U.S. PIRG EDUC. FUND (Feb. 2024), https://epic.org/state-of-privacy.

[3] Maryland Online Data Privacy Act of 2024, S.B. 541, 2024 Leg., 446th Sess. (Md. 2024).

[4] Press Release, Cal. Priv. Prot. Agency, CPPA Applauds Governor Newsom for Approving the California Delete Act (Oct. 11, 2023), https://cppa.ca.gov/announcements/2023/20231011.html.

[5] Washington My Health My Data Act, ch. 191, 2023 Wash. Sess. Laws 867.

[6] *See* 740 ILL. COMP. STAT. 14/ (2008).

[7] *See, e.g.*, S. 148, 193d Gen. Ct. (Mass. 2023).

considering how to regulate AI and other technologies, like facial recognition, that can enable discrimination, fraud, or other harms.

But we must also recognize that while residents of some states may enjoy data protections, they are the minority. Nationwide, people in most jurisdictions are being left behind.

Any new federal legislation must account for both evolving protections and gaps at the state level. This new bill must be at least as strong as the state laws to justify any form of preemption that would restrict the states from continuing in their role as the "laboratories of democracy." And it needs to extend protections nationally, so the entire country benefits.

The American Privacy Rights Act represents an imperfect but needed bargain to protect everyone's rights amid this patchwork landscape. Who we are and how we behave can be collected, analyzed, and exploited by companies at home and by nations abroad. Nationwide, people are harmed everyday by algorithmic discrimination, fraud, stalking, and other abuses fueled by the invasion of our privacy. Consumer data fuels disinformation campaigns by foreign adversaries who seek to undermine American democracy. Comprehensive privacy protection is also necessary to mitigate risks to individuals from artificial intelligence. If personal data is the new oil, AI and other algorithmic technologies represent a new form of combustion. Time is short and stakes are high; we must require these new technologies to be safe and effective from the outset, lest they blow up in our face.

Overall, we're highly encouraged by the following provisions in the new bill. But we also urge the Committee to consider key fixes and improvements.

First, the bill would prohibit discriminatory uses of personal data and require companies to test their algorithms for bias. Years of reporting and research show that algorithms used for advertising, pricing, and eligibility decisions frequently produce discriminatory outcomes across critical areas of the economy. A review of over two million mortgage applications found that Black applicants were 80 percent more likely to be rejected by mortgage approval algorithms when compared with similar white applicants.[8] Scoring algorithms used by auto insurers judge applicants "less on driving habits and increasingly on socioeconomic factors."[9] When an algorithm executes its mission of creating efficiency by finding hidden correlations amid large sets of data, it will often mistake the long-term consequences of discrimination and

[8] Emmanuel Martinez & Lauren Kirchner*, The Secret Bias Hidden in Mortgage-Approval Algorithms*, THE MARKUP (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

[9] CONSUMER REPS., *The Truth About Car Insurance* (July 30, 2015), https://www.consumerreports.org/cro/car-insurance/auto-insurance-special-report/index.htm.

inequality for an individual's preferences and traits.[10] These mistaken shortcuts fail to account for the fact that while a person may be in part a product of their circumstances, that does not mean they necessarily *are* or *should be* limited by those circumstances. Expediency is no excuse for segregation.

This discrimination disproportionately impacts Black people and other people of color, including people with intersectional identities, like immigrants, women of color, and LGBTQI+ people of color.[11] However, the current language in the anti-discrimination provision contains an exception which could unintentionally allow advertising, marketing, or soliciting that segregates base on racial groups and populations. If a business posts a sign that says, "Whites Only", it should not matter whether it is written in ink or pixels, words, or code. The discrimination and harm are the same. The legal consequences should be the same too. We believe fixing this provision is an easy but important action to secure the core intent of the American Privacy Rights Act.

Second, the bill would require companies to collect and use only as much personal data as is necessary, proportionate, and limited to provide the services that consumers expect, and to safeguard that data. This builds consumer trust and reduces the risk of personal data being exploited for fraud, theft, and deceptive practices. Identity theft and fraud disproportionately impact communities of color, and low-income consumers are less likely to have the resources to bounce back after being ripped off.[12] Data limitations and privacy rules create a bedrock level of trust for consumers, who can better make choices about how to interact and allow their data to be used when they know what to expect. However, we are concerned that this bill has backtracked from ADPPA by removing the right of individuals to bring claims based on violations of the rules governing the collection, processing, and retention of sensitive covered data. We also believe that the advertising provisions need clarification to avoid confusion for businesses and consumers alike. Additionally, service providers for government entities need to be covered by the bill, as they were in ADPPA, to avoid potential loopholes and gamesmanship.

[10] *See generally* WHITE HOUSE OFF. OF SCI. & TECH. POL'Y, BLUEPRINT FOR AN AI BILL OF RIGHTS 24–25 (2022) [hereinafter *Blueprint*], https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf; Jane Chung, *Racism In, Racism Out: A Primer on Algorithmic Racism*, PUBLIC CITIZEN (2022), https://www.citizen.org/article/algorithmic-racism/; Yeshimabeit Milner & Amy Traub, *Data Capitalism and Algorithmic Racism*, DATA FOR BLACK LIVES & DEMOS (2021), https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf.

[11] *See* CHUNG, *supra* note 10, at 10; MILLNER & TRAUB, *supra* note 10.

[12] FTC, SERVING COMMUNITIES OF COLOR: A STAFF REPORT ON THE FEDERAL TRADE COMMISSION'S EFFORTS TO ADDRESS FRAUD AND CONSUMER ISSUES AFFECTING COMMUNITIES OF COLOR (2021), https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf.

Third, the bill would give individuals transparency into and control over how their data is used while prohibiting "dark patterns"—some of the worst practices that trick individuals into unwittingly divulging data and create design barriers that prevent individuals from exercising their rights. The bill clearly empowers individuals with the ability to access, correct, delete, and port their own information. Yet, parts of the bill could undermine protections enforced by other federal agencies. For example, the bill's displacement of the Communications Act is vague and overbroad. This will have serious, possibly unintended consequences, including endangering the FCC's consumer protection authorities as well as its work to combat illegal robocalls. At the Lawyers' Committee, we have worked for years to fight voter intimidation robocalls in particular.[13] We do not think the drafters intended to protect individuals from abusive practices online but condemn them to more fraudulent or exploitative practices over the phone. Additionally, individuals should have peace of mind when they consent to transfer their data. Currently, the APRA could allow one agreed data transfer from an individual to mean that all the data they transferred is open to resale to third parties. Data brokers should have clear obligations to individuals and to each other. The APRA could be improved to protect the subsequent spread of sensitive information once it is initially transferred.

Lastly, we applaud the meaningful enforcement authority that this bill vests in federal, state, and individual actors. Having a private right of action allows individuals to obtain relief from a court when a company violates the Act. The ability to bring a private lawsuit is particularly important for communities of color that, historically, could not rely on the government to vindicate their rights. That is why practically every major civil rights law has a private right of action. A right without a remedy is no right at all to people who have been wronged.

In addition, the bill gives many new responsibilities and authorities to the Federal Trade Commission, as it should. The FTC, however, has been underfunded for decades.[14] A mandate for a new bureau, especially one "...comparable in structure, size, organization, and authority to the existing bureaus within the Commission related to consumer protection and competition" must be paired with new resources, or else privacy enforcement from the federal government be hamstrung from the get-go. It is imperative for Congress to ensure that the FTC receives the resources it needs to successfully execute this new mission.

We have long said that when it comes to privacy legislation, we cannot afford to make the perfect the enemy of the good. In a strong compromise that can stand the

[13] *See Nat'l Coal. on Black Civic Participation v. Wohl (NCBCP I)*, 498 F.Supp. 3d 457, 464 (S.D.N.Y. 2020); *Nat'l Coal. on Black Civic Participation v. Wohl (NCBCP III)*, 661 F. Supp. 3d 78 (2023).

[14] Justin Sherman, *The Key to Protecting Privacy Is Locked in an Underfunded Government Agency*, SLATE (July 14, 2023), https://slate.com/technology/2023/07/federal-trade-commission-funding-privacy.html.

test of time, no one gets everything they want. There are parts of this bill that we do not like. But millions in this nation—disproportionately Black people and other people of color—currently face severe and ongoing harms from the invasion of their privacy, including discrimination, stalking, fraud, and other exploitative data practices. Those individuals, and this Congress, cannot afford to wait.

Almost sixty years ago, we decided as a nation that our polity is stronger when everyone has a fair chance. Congress passed the Civil Rights Act of 1964 to prohibit segregation in interstate commerce. Today, advanced technologies have created both new opportunities and new forms of insidious discrimination. The internet is not coded on a blank slate. The future of equal opportunity depends on whether we prevent the data-driven economy of the 21st century from replicating the mistakes of the past. The promise of the internet, and the democratic aspirations imbued in its creation, depend on it. It is time for Congress to act.

II. Lack of Privacy and Online Civil Rights Protections Enable Algorthmic Discrimination Across the Economy

Equal opportunity, privacy, and civil rights are intertwined with technological advancement. Algorithms use data to make decisions about all aspects of peoples' lives, determining who can rent a house, who can get a loan, who can get a deal, and consequentially—who cannot. One of the greatest civil rights challenges of our generation is to ensure that our new data-driven economy does not replicate or amplify existing discrimination. To ensure that technology serves all of us. But achieving the full measure of freedom in a data-driven economy also requires freedom from discrimination, which is increasingly amplified online through algorithmic bias and pervasive data collection.

Although algorithmic systems are widely used, they pose a high risk of discrimination, disproportionately harming Black communities and other communities of color. Because these algorithmic technologies are typically built using societal data that reflects generations of discriminatory practices such as redlining and segregation, they often replicate and reinforce past patterns of discrimination. The tools of the future lock us into the mistakes of the past.

Commercial surveillance, data collection, and algorithmic decision-making reinforce a separate and unequal society, and correspondingly an unequal market. Each click, habit, and individual characteristic is collected and cataloged to discern not just preferences, but sensitive data about individuals' race, religion, gender, and other traits—or proxies for them. Algorithmic systems use this information to determine what products consumers see, what price or interest rate they are quoted, and what eligibility they qualify for.

Privacy legislation is a civil rights issue because privacy protections can help ensure that people's identities and characteristics cannot be used against them unfairly. Such protections can empower communities of color and open doors for marginalized populations. It can also provide clarity to businesses and level the playing field for entrepreneurs.

However, there is currently no comprehensive federal privacy law. Existing anti-discrimination laws have many gaps and limitations as well. Some exclude retail or have unresolved questions as to whether they apply to online businesses. Others apply to specific sectors, like housing and employment, but may not cover new types of online services used to match individuals to these opportunities. To give a few examples, under current federal civil rights law it would be legal for an online retailer to charge higher prices to women or to refuse to sell products to Christians.[15] A service provider could use discriminatory algorithms to look for workers to target for recruitment so long as the provider does not meet the definition of an "employment agency" under Title VII.[16] And it is wholly unclear whether existing laws will apply at all to discrimination in many new online-only economies related to online gaming, influencers, streamers, and other creators.

As a result of gaps in federal law, individuals currently have little recourse against a modern barrage of discriminatory algorithmic tools. The race for more advanced models builds a demand for more data, and correspondingly more surveillance of consumers, regardless of whether these commercial data practices reinforce the structural racism and systemic bias that pervade our society. Tech companies have every incentive to misuse personal data, intentionally or unintentionally, in ways that harm historically marginalized communities through deception, discrimination, exploitation, and perpetuation of redlining. Without a strong privacy standard, companies holding personal data can use it to directly discriminate against people of color or other marginalized groups. They can also make data available to other actors who use it to discriminate, or design data processing practices in a manner that negligently, recklessly, or knowingly causes discriminatory or otherwise harmful results, such as algorithmic bias or promotion of disinformation.[17]

[15] *See* 42 U.S.C. §§ 1981, 2000a; *Shaare Tefila Congregation v. Cobb*, 481 U.S. 615 (1987) (noting that Sec. 1981 does not apply to sex discrimination or religious discrimination unless discrimination against Jews or Arab Muslims).

[16] Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN (Dec. 10, 2018), https://www.upturn.org/work/help-wanted/.

[17] As one court observed in a 2020 case involving voter intimidation robocalls targeted at Black communities:

(footnotes continue on next page)

The bottom line is that if these companies and data brokers were not collecting, aggregating, and using vast quantities of personal data in privacy-invasive ways in the first place, many of these harms would not happen or would be far more difficult to execute.

Not surprisingly, extensive documentation cited in the attached appendix demonstrates that exploitative data practices enable worse treatment of Black people and other historically marginalized communities and unequal access to goods and services due to discriminatory algorithms across sectors of the economy that include housing, employment, credit and finance, insurance, healthcare, education, retail, and public accommodations.

For example, online real estate brokerage Redfin was sued for engaging in redlining in violation of the Fair Housing Act. Redfin offered limited service to homes under a certain price, which depressed sale prices. The National Fair Housing Alliance found this policy varied in different cities and had a racially disparate impact, discriminating against buyers and sellers of homes in communities of color.[18]

Similarly, in the property rental market—which families of color are disproportionately likely to use—some of the largest property managers in the country use software company RealPage's rent-setting algorithm. The algorithm allegedly draws on private data, including the rent prices that local competitors charge, to inflate prices and stifle market competition through its rent recommendations.[19]

> Today, almost 150 years later, the forces and conflicts that animated Congress's adoption of the Ku Klux Klan Act as well as subsequent voting rights legislation, are playing out again before this Court, though with a difference. In the current version of events, the means Defendants use to intimidate voters, though born of fear and similarly powered by hate, are not guns, torches, burning crosses, and other dire methods perpetrated under the cover of white hoods. Rather, Defendants carry out electoral terror using telephones, computers, and modern technology adapted to serve the same deleterious ends. Because of the vastly greater population they can reach instantly with false and dreadful information, contemporary means of voter intimidation may be more detrimental to free elections than the approaches taken for that purpose in past eras, and hence call for swift and effective judicial relief.

NCBCP I, 498 F.Supp. 3d at 464.

[18] Associated Press, *Redfin to Pay $4 Million to Settle Lawsuit Alleging Housing Discrimination*, MARKETWATCH (May 2, 2022), https://www.marketwatch.com/story/redfin-to-pay-4-million-to-settle-lawsuit-alleging-housing-discrimination-01651500520.

[19] Heather Vogell et al., *Rent Going Up? One Company's Algorithm Could Be Why*, PROPUBLICA (Oct. 15, 2022), https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent; Heather Vogell, *Senators Had Questions for the Maker of a Rent-Setting Algorithm. The Answers Were "Alarming."*, PROPUBLICA (Mar. 21, 2023), https://www.propublica.org/article/yieldstar-rent-increase-realpage-warren-sanders.

In lending, too often a consumer's identity will determine which products they are offered. Google's search engine has served users targeted ads for payday loans when they ran searches for terms associated with financial distress, such as "[I] need money to pay my rent."[20] Data used to score consumers' credit has been shown to be capable of predicting the race and gender of loan applicants.[21] Another study found that biases in "algorithmic strategic pricing" resulted in Black and Latino borrowers paying higher interest rates on home purchase and refinance loans, amounting to $250–$500 million annually.[22] These pricing disparities are commonly driven by machine learning algorithms that target customers based on their personal data.

Algorithmic discrimination is also increasingly manifesting in retail settings. For eight years, Rite Aid pharmacies used discriminatory and inaccurate facial recognition technology that erroneously accused customers of shoplifting and falsely flagged women and people of color at higher rates.[23] Studies show facial recognition algorithms misidentify people of color and women at higher rates than white, male faces,[24] yet they are increasingly used in groceries stores and shopping malls across the country.[25] Because of historical redlining and segregation, and the lack of retail options in many low-income neighborhoods, low-income communities of color often pay higher prices than wealthier, whiter neighborhoods when they shopped online. For example, algorithms that distribute discount-related ads tend to direct those ads

[20] Aaron Reike & Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, UPTURN 15 (Oct. 2015), https://www.upturn.org/work/led-astray-online-lead-generation-and-payday-loans/.

[21] *See* Bertrand K. Hassani, *Societal Bias Reinforcement Through Machine Learning: A Credit Scoring Perspective*, 1 AI & Ethics 239 (2020), https://link.springer.com/article/10.1007/s43681-020-00026-z.

[22] Laura Counts, *Minority Homebuyers Face Widespread Statistical Lending Discrimination, Study Finds*, U.C. Berkeley Haas Sch. of Bus. (Nov. 13, 2018), https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/.

[23] Press Release, FTC, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

[24] Press Release, Nat'l Inst. of Standards & Tech., NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[25] Kristie Keleshian, *Facial Recognition Technology Used at New York Supermarkets Raises Some Questions About Privacy*, CBS NEWS (Mar. 18, 2023), https://www.cbsnews.com/newyork/news/new-york-city-grocery-stores-supermarkets-facial-recognition-cameras/; Rebecca Heilweil, *From Macy's to Albertsons, Facial Recognition Is Already Everywhere*, VOX (July 19, 2021), https://www.vox.com/2021/7/15/22577876/macys-fight-for-the-future-facial-recognition-artificial-intelligence-stores.

toward high-income white users.[26] Service is also affected. Amazon's same-day delivery service excluded predominantly Black zip codes in Atlanta, Boston, Chicago, Dallas, New York, and Washington. For example, in Boston, three zip codes in the primarily Black neighborhood of Roxbury were excluded from same-day service, but the neighborhoods surrounding Roxbury on all sides were eligible.[27]

Meanwhile, discrimination based on data is used to exclude educational opportunities. Naviance college admissions software, used by approximately two-thirds of high schoolers, allows colleges to target ads to prospective students on the basis of race and location. An investigation found examples of some universities, including the University of Kansas, University of Southern Maine, and University of Massachusetts Boston, deliberately—sometimes exclusively—advertising to white students.[28] The common denominator in all of these examples is sloppy or abusive use of personal data. By prohibiting discriminatory data use and requiring companies to test their algorithms for bias, many of these harms can be prevented.

III. The American Privacy Rights Act

The "American Privacy Rights Act" would establish a national data privacy and data security framework. We are pleased to see that it prioritizes civil rights protections that address data-driven discrimination. The draft legislation is a significant step towards enacting a major comprehensive privacy proposal which can gain bipartisan and bicameral support. We are encouraged by the progress of this legislation and want to address this Committee on the core strengths of this discussion draft and needed improvements to capitalize on those strengths.

A. *Welcomed Civil Rights Protections and Needed Fixes*

It is past time to enact a comprehensive consumer privacy law that safeguards civil rights online. Congress has failed to enact comprehensive privacy legislation despite many attempts since the beginning of the millennium.[29] We are encouraged by the strong civil rights section of the American Privacy Rights Act especially the language that seeks to change the status quo for Americans harmed by discriminatory algorithms, advertising, and retail discrimination. The need is

[26] Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, HARV. BUS. REV. (Nov. 8, 2019), https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias).
[27] David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERG (Apr. 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day/.
[28] Todd Feathers, *College Prep Software Naviance Is Selling Advertising Access to Millions of Students*, THE MARKUP (Jan. 13, 2022), https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students.
[29] *See, e.g.*, Patrick Thibodeau, FTC, Senator Seek Online Privacy Rules, COMPUTERWORLD (May 26, 2000), https://www.computerworld.com/article/1373941/ftc-senator-seek-online-privacy-rules.html

pressing. As a result of federal absence, existing civil rights laws do not cover the entirety of the discriminatory harms people routinely experience online.

We welcome the civil rights provisions of the "American Privacy Rights Act" that will prohibit many common forms of online discrimination. The bill prohibits using personal data to discriminate based on protected characteristics. It would also apply to discriminatory algorithms and technologies that use them, such as commercial uses of biased facial recognition systems.[30] The bill allows companies to process protected class data for the purpose of self-testing to root out discrimination, or to expand the pool of applicants, candidates, or customers. The anti-discrimination provision would also preserve free speech; it does not apply to non-commercial activities or to private clubs or groups, which are the same exceptions in the Civil Rights Act of 1964.

However, the addition of a clause in the bill exempting "advertising, marketing, or soliciting economic opportunities or benefits to underrepresented populations or members of protected classes" is rife for abuse. *This provision needs to be deleted*. First, underrepresentation is undefined in the Act and completely depends on context. An advertiser could combine multiple identity traits and jerry rig the relevant target market to make almost any demographic appear "underrepresented." Second, the provision directly allows advertising and solicitations to be targeted to specific protected classes. Because of the nature of online targeted advertising, this means that other groups who are not in the target audience would be excluded from receiving those opportunities. This would allow "whites only" retail ads or "men only" financial services ads, for example. This is precisely the type of conduct that caused the Department of Justice to sue Facebook for violating the Fair Housing Act.[31] On the internet, ads and promoted content are often the primary vehicle for discovering a product or service. However well intentioned this clause may be, it is a dangerous backdoor to a return of de facto commercial segregation.

On a more positive note, the civil rights provision in the bill will also apply to social media platforms. These protections should help increase fairness in recommendation algorithms that have been shown to disadvantage creators and

[30] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[31] *See* Press Release, U.S. Dep't of Just., 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.

influencers of color.[32] These provisions are critical in addressing civil rights online. We are encouraged by the digital access rights and transparency requirements that will help identify discriminatory practices, and we urge this Committee to make needed light touch fixes and include strong civil rights protections in legislation going forward.

B. *Opportunity to Improve Algorithmic Assessments*

In addition, the bill requires pre-deployment algorithmic design evaluations and post-deployment impact assessments for the algorithms employed by covered entities. We have seen algorithms reproduce patterns of discrimination in employment recruiting, housing, education, finance, mortgage lending, credit scoring, healthcare, vacation rentals, ridesharing, and other services.[33] We applaud that the bill requires the assessments to test for discrimination in these types of economic opportunities, as well as to explicitly test for disparate impacts on the basis of protected characteristics.

However, there is a large opportunity to improve this section based on learnings about data practices and AI development over the past few years. In particular, the Lawyers' Committee prefers a regulatory structure that assigns different and detailed requirements for developers and deployers of algorithms, to recognize their different roles. Developers are often better situated to assess design issues, while deployers often are better situated to assess implementation issues. As currently written, it could be difficult for a developer who is not a deployer, or vice versa, to comply with the requirements.

We recommend modifying or replacing this subsection with more precise mandates, such as in the Lawyers' Committee's own model legislation, the "Online Civil Rights Act."[34] This will lead to more prescriptive assessments of algorithmic tools both before and after deployment, while also giving clearer guidance to industry and more tailored requirements for those building innovative technologies on top of large personal data sets.

We also support redefining the covered algorithm definition and consequential decision definition, so that algorithmic tools are evaluated based on their ability and

[32] Reed Albergotti, *Black Creators Sue YouTube, Alleging Racial Discrimination,* WASH. POST (June 18, 2020), https://www.washingtonpost.com/technology/2020/06/18/black-creators-sue-youtube-alleged-race-discrimination/; *Twitter Finds Racial Bias in Image-cropping AI*, BBC (May 20, 2021), https://www.bbc.com/news/technology-57192898.

[33] Letter from Civil Rights, Civil Liberties, and Consumer Protection Organizations to the FTC (Aug. 4, 2021), https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf.

[34] *See* Lawyers' Committee for Civil Rights Under Law, *Online Civil Rights Act* (model legislation) § 102 (Dec. 2023), https://www.lawyerscommittee.org/wp-content/uploads/2023/12/LCCRUL-Model-AI-Bill.pdf.

likelihood to impact the critical areas of life that matter to individuals. At present, the definition of covered algorithm is critically broken. It would sweep up *any* computational process—i.e. any use of a computer. This would subject many extremely basic or unobjectionable forms of computation to provisions that use this term, such as the algorithmic impact assessments. Following the model of our Online Civil Rights Act, we recommend defining "covered algorithm" more narrowly to focus on technologies like AI and machine learning, and also tying the definition to circumstances involving "consequential actions."

These revisions would mandate that developers and deployers of algorithmic tools, like AI systems, should be required to evaluate and audit their products for discrimination, bias, and harm both before and after deploying or offering their products in interstate commerce. First, developers and deployers should be required to conduct a short form evaluation checking whether it is plausible that the use of an algorithm may result in a covered harm under the act. If harm isn't plausible, they should be free from further regulatory requirements.

If harm is plausible, the legislation should require developers and deployers to engage an independent auditor to evaluate the algorithm's design, how it makes or contributes to decisions about significant life opportunities, how the algorithm might produce harm and how that harm can be mitigated. Deployers should then annually assess the algorithm as it is used, detailing any changes in its use or any harms it produces, including measuring disparate impacts. Developers should review these assessments to determine if the algorithm needs modifications, and the evaluations, assessments, and reviews should be publicly shared and reported to a federal regulator. Sunlight is the best disinfectant.[35] The evaluation should include a detailed review and description so that external researchers can evaluate how the covered algorithm functions, including its risks, uses, benefits, limitations, and other pertinent attributes. Both evaluations and assessments should be reported to the Federal Trade Commission and summarized on the websites of developers and deployers.

C. *Important Data Minimization Standards*

Pervasive access to peoples' personal data, often obtained without the knowledge or consent of the individual, can lead to discriminatory, predatory, and unsafe practices. The internet is rife with examples of how the overcollection of data leads to unsafe conditions for people of color or particularly vulnerable individuals. Companies should not collect or use more personal info than is necessary to do what the individual expects them to do. Beyond basic cybersecurity and legal obligations,

[35] *See* Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WEEKLY 11 (Dec. 20, 1913) ("Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.").

companies also should not use personal data for secondary purposes that an individual does not expect or has not consented to. The reason is simple: personal data collected by companies can proliferate in a way that maximizes risk for the individual and for society at-large. This has become glaringly apparent to those seeking reproductive health care or seeking to protect Black children from online abuses.

For example, data broker SafeGraph collected, packaged, and sold location data specifically tracking visitors to over 600 Planned Parenthood locations,[36] while Meta has collected sensitive patient information from healthcare and hospital websites, including data on people seeking abortions and to have children.[37] It collected health information, including ovulation data, from health apps without user consent.[38]

Data about users on YouTube, Meta, and TikTok all contributes to the development of algorithms that have been alleged to recommend content that engage in racial profiling and disproportionately push violent, drug-filled, and sexual content to Black youth, including content driving Black kids to engage in self-harm.[39] Data about Black children has also been used to deliver predictions that disproportionately flag Black children for a "mandatory" neglect investigation in child welfare agencies, or as high risk in school setting, when compared with white children.[40]

[36] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE: MOTHERBOARD (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

[37] *See* Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (June 5, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients; Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook*, THE MARKUP (June 21, 2022), https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook; Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[38] Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[39] BUSINESSWIRE, *Social Media Victims Law Center Files Suit Against Social Media Giants for the Race-Driven Anguish Suffered by One Small-Town Family* (Aug. 2, 2022), https://www.businesswire.com/news/home/20220802005949/en/Social-Media-Victims-Law-Center-Files-Suit-Against-Social-Media-Giants-for-the-Race-Driven-Anguish-Suffered-by-One-Small-Town-Family; Sharyn Alfonsi, *More than 1,200 Families Suing Social Media Companies Over Kids' Mental Health*, CBS NEWS (Dec. 11, 2022), https://www.cbsnews.com/news/social-media-lawsuit-meta-tiktok-facebook-instagram-60-minutes-2022-12-11/.

[40] *See* Sally Ho & Garance Burke, *An Algorithm That Screens for Child Neglect Raises Concerns*, AP NEWS (Apr. 29, 2022), https://apnews.com/article/child-welfare-algorithm-investigation-9497ee937e0053ad4144a86c68241ef1; Todd Feathers, *False Alarm: How Wisconsin Uses Race and Income to Label Students "High Risk"*, THE MARKUP (May 11, 2023), https://themarkup.org/machine-learning/2023/04/27/false-alarm-how-wisconsin-uses-race-and-income-to-label-students-high-risk.

Clear baseline protections for data collection, including both primary and secondary uses of data, should be enacted to help cage these types of risks, and prevent harms. Personal data are the fuel of online commerce. They can be used for good—to create new products, conduct beneficial research, mitigate disparities, or tailor experiences that consumers want. They can also be abused—to steal someone's identity, exclude someone from opportunities, target someone for harassment or abuse, engage in predatory practices and scams, or to reinforce legacies of segregation and redlining. Keeping data collection, use, and sharing limited to what is necessary, proportionate, and limited to provide expected services is essential to keeping consumers safe.

This Act reduces the amount of data that will fall into the wrong hands, providing a knock-on benefit in combating illicit fraud and identity theft. Data breaches are often especially problematic for people of color living on fixed or low incomes.[41] Companies track cell phone location data without consent and sell this data to debt collectors and other predatory actors, which disproportionately harms low income Black and Brown communities.[42] This bill's data minimization requirements will restrict data collection and use to purposes necessary for providing services expected by an individual and restricts secondary uses or data sharing without explicit opt-in consent. Importantly, the bill imposes tighter protections for "sensitive covered data," such as restricting its use for advertising. However, the data minimization requirements should also be enforceable by a private right of action. The private right of action in the APRA, while generally praiseworthy, does not apply to the data minimization section of the bill, which is a core protection for consumers. This means individuals will not be able to sue when a company fails to comply with their most basic requirement to only process personal data in a manner that is necessary and proportionate.

We are encouraged that the Act imposes a baseline duty on all covered entities to collect or use covered data only as needed and appropriate. It does not create a "notice and consent" regime in which any practice is allowed so long as a consumer consents after being presented with lengthy and legalistic privacy notices. Notice and consent has repeatedly been shown to be a failure. We do not allow individuals to consent to more arsenic in their drinking water or opt-out of smoke alarms in their homes. We do not expect consumers to inspect a car's engine before driving it off the sales lot. Rather, we impose baseline protections so that consumers can trust that

[41] Kori Hale, *T-Mobile's Hack of 50 Million Users Leaves Black Community at Risk*, FORBES (Sept. 9, 2021), https://www.forbes.com/sites/korihale/2021/09/10/t-mobiles-hack-of-50-million-users-leaves-black-community-at-risk/.

[42] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, VICE NEWS*,* (Jan. 8, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

products are safe and functional without having to look under the hood. Consumers should expect no less from digital products.

D. Individual Empowerment through Transparency and Control

Transparency about how companies collect and use data will ultimately shed light on discriminatory practices. Providing individuals with understandable, easy to read, privacy policies detailing data collection puts the individual in the driver's seat. This transparency, coupled with giving users the ability to access, correct, or delete their data, lets individuals make empowered choices. They can choose to access and correct their data, opening pathways to self-sufficient fixes for inaccurate background check reports, which disproportionately harm Black and Brown people.[43] Provisions contained in the American Privacy Rights Act give individuals the power to delete their data and empower them to protect themselves. They can reduce their data footprint, or take away their data from insecure third parties, minimizing the risk of fraud, identify theft, and exploitation. Or they can port their data to another company that will give them better service.

Additionally, new provisions boost individual autonomy, including a prohibition on "dark pattern" user interfaces designed to thwart decision making and deceive and deprive users of the choices they hold. This addition is to be applauded and protected. Likewise, the prohibition on pre-dispute arbitration agreements for those under the age of 18 or alleging a substantial privacy harm—which includes harms from discrimination—also works to empower individuals. Individuals should not be denied access to a court of law when seeking to protect their privacy or the privacy of their children.

Requirements on third parties who buy, sell, and collect data, also known colloquially as data brokers, also work to empower individuals and increase transparency. Currently, data brokers continually collect and amass data for sale. Some may not be accurate. Most individuals are unaware what information is bought or collected about them. This data is then used to conduct background checks for employment, housing, and other services, as well as for credit scoring. Inaccuracies disproportionately harm people of color, as well as those who have a conviction or arrest record—even if that arrest never resulted in a conviction. This bill rectifies that harm by creating a data broker registry, reporting requirements, and a national opt-out registry. In addition, the bill requires businesses—including data brokers—

[43] Christina Stacy & Mychal Cohen, *Ban the Box and Racial Discrimination: A Review of the Evidence and Policy Recommendations*, URBAN INST. 17 (Feb. 2017), https://www.urban.org/sites/default/files/publication/88366/ban_the_box_and_racial_discrimination_4.pdf (finding that inaccuracies in criminal record data especially harm people of color, because they represent a disproportionate share of U.S. arrests and are thus more likely to have missing information regarding the outcome of a case).

to minimize the data they collect, restricts selling such data to third parties without consent, and provides individuals with a right to access, correct, or delete their data.

However, the American Privacy Rights Act should tread carefully. We see two problems with current provisions regarding data brokers. *First*, the Consumer Financial Protection Bureau is currently planning to propose a rule which would designate data brokers as credit reporting agencies due to the vast amounts of financial data on individuals that they collect. This would make data brokers subject to the requirements of the Financial Credit Reporting Act (FCRA).[44] As currently drafted, the American Privacy Rights Act would turn this designation into a trapdoor, allowing data brokers designated as credit reporting agencies to fall out of the scope of this legislation under a broad carve out for institutions regulated by FCRA. This loophole should be closed by more carefully tailoring the FCRA exemption. Data brokers with vast troves of financial data and personal information are exactly the type of actor this Act should aim to regulate. This bill will provide additional protections above and beyond what CFPB is doing and will reduce uncertainty for businesses by doing it in a statute.

Second, broad carve outs for service providers in different contexts could undermine enforcement and empowerment. Data brokers acting as service providers to a government entity are not covered by the current draft of the Act. This was not the case in ADPPA, which did apply to this category of service providers. Ad-tech companies and data brokers also have a recent history of attempting to exploit "service provider" exemptions to continue to exploit individual's data.

E. *Making Privacy Rights Real Through Real Enforcement.*

As encouraged as we are about some provisions of this Act, we know that data privacy legislation will only live up to its promise if it is able to be readily enforced. We are encouraged that the American Privacy Rights Act gives clear enforcement authority to federal, state and individual actors. The best way for an individual to safeguard their rights is to be able to seek a remedy to the injury they suffer themselves, in a court of law. This private right of action must be protected and expanded to include core data minimization sections of APRA as this legislation advances.

However, there is more to be done to make the promise of this legislation real for the individuals and agencies that would enforce it. As mentioned, the Federal Trade Commission has been historically under resourced. Creating a privacy bureau

[44] Press Release, Consumer Fin. Prot. Bureau, CFPB Launches Inquiry Into the Business Practices of Data Brokers (Mar. 15, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/.

within the FTC would require, at minimum, substantial new funding, and likely stronger enforcement tools.

IV. Conclusion

The “American Privacy Rights Act” is a promising piece of legislation aimed at solving long lingering critical problems. We appreciate this Committee’s continued attention to the issue and the opportunity to testify on how to strengthen privacy protections for individuals and curb data-driven discrimination. The Lawyers’ Committee looks forward to working on a bipartisan basis to strengthen this bill so that it could advance over the finish line, ultimately securing long overdue data privacy and online civil rights protections for all people, particularly Black people and other people of color who are most often targeted for harm in the digital world.

Appendix I: Commercial Surveillance and Algorithmic Harms Impacting Black Communities and Other Communities of Color

This appendix catalogues extensive evidence of the disparate harms and unequal access to goods and services that consumers of color continue to face due to discriminatory algorithms and exploitative data practices. This spiral of inequality is pervasive across all sectors of our economy and daily life: housing, employment, credit and finance, insurance, healthcare, education, retail, and public accommodations. Even where commercial surveillance and algorithmic harms extend beyond the economy, into voting, government services, and policing, they are frequently the result of companies pursuing a no-holds-barred strategy to outpace their competition, with reckless disregard for consumer rights and civil rights; and once these companies succeed in controlling the market, they face little to no pressure to mitigate such harms. It is ultimately Black and Brown consumers who suffer from these market inequities and destructive externalities.

A. Housing

- Mortgage approval algorithms denied applications from homebuyers of color substantially more than white homebuyers. A review of over two million conventional mortgage applications found that, nationally, "lenders were 40 percent more likely to turn down Latino applicants for loans, 50 percent more likely to deny Asian/Pacific Islander applicants, and 70 percent more likely to deny Native American applicants than similar White applicants. Lenders were 80 percent more likely to reject Black applicants than similar White applicants."[1] Lenders used formulas mandated by Fannie Mae and Freddie Mac, which were known to be detrimental to people of color.[2]

- Meta recently settled a housing discrimination lawsuit brought by the Department of Justice and Department of Housing and Urban Development, which alleged that Facebook's advertising targeting and delivery mechanisms discriminated on the basis of race and other protected characteristics—including

[1] Emmanuel Martinez & Lauren Kirchner*, The Secret Bias Hidden in Mortgage-Approval Algorithms*, THE MARKUP & ASSOCIATED PRESS (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

[2] *Id.*

literal redlining.[3] Meta agreed to create a new system to reduce disparities in the delivery of housing ads as part of the settlement.[4] Facebook has also been sued by civil rights advocates for similar conduct and causes of action.[5]

- This settlement came after years of reports and research showing that Facebook's advertising system both allows discriminatory targeting and algorithmically delivers ads in a discriminatory fashion—issues that have persisted despite

[3] *See* U.S. Dep't of Just., *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; Charge of Discrimination at 4, *U.S. Dep't of Hous. & Urban Dev. v. Facebook, Inc.*, FHEO No. 01-18-0323-8 (Mar. 28, 2019); *see also* Brief of *Amicus Curiae* Lawyers' Committee for Civil Rights Under Law in Support of Plaintiff's Opposition to Facebook's Demurrer to First Amended Complaint at 10, *Liapes v. Facebook, Inc.*, Case No. 30-CIV-01712 (Cal. Super. Ct. Mar. 5, 2021), https://lawyerscommittee.org/wp-content/uploads/2021/03/Leave-and-Amicus-Combined.pdf.

[4] *See* Salvador Rodriguez, *Facebook Starts Effort to Boost Equity in Housing Ads*, WALL ST. J. (Jan. 9, 2023), https://www.wsj.com/articles/facebook-starts-effort-to-improve-equity-in-housing-ads-11673294404.

[5] *See* Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU (Mar. 19, 2019), https://www.aclu.org/news/womens-rights/facebook-settles-civil-rights-cases-making-sweeping.

promises to address the problem.[6] Facebook's own civil rights auditors called out the risk of algorithmic bias in its advertising system.[7]

- Google and Twitter have both been investigated by HUD for similarly discriminating in housing advertisements in violation of the Fair Housing Act.[8]

- Public housing facilities across the country are using facial recognition technologies to monitor resident behavior, despite significant evidence showing that such technologies are significantly less accurate when used to identify women, Black people, and other people of color. The growing use of these tools disproportionately subjects Black people, other people of color, and low-income communities to round-the-clock surveillance that often leads to increased contact with law enforcement, which can be especially dangerous when false-positive identifications lead to wrongful arrests.[9]

[6] **Discriminatory Targeting:** Angie Waller, *Facebook Says It's Dropped "Sensitive" Ad Targeting Categories*, THE MARKUP (Jan. 25, 2022), https://themarkup.org/newsletter/citizen-browser/facebook-says-its-dropped-sensitive-ad-targeting-categories; Jinyan Zang, *Solving the Problem of Racially Discriminatory Advertising on Facebook*, BROOKINGS (Oct. 19, 2021), https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/; Jon Keegan, *Facebook Got Rid of Racial Ad Categories. Or Did It?*, THE MARKUP (July 9, 2021), https://themarkup.org/citizen-browser/2021/07/09/facebook-got-rid-of-racial-ad-categories-or-did-it; Jeremy B. Merrill, *Does Facebook Still Sell Discriminatory Ads?*, THE MARKUP (Aug. 25, 2020), https://themarkup.org/the-breakdown/2020/08/25/does-facebook-still-sell-discriminatory-ads; Barbara Ortutay, *Facebook to Overhaul Ad Targeting to Prevent Discrimination*, ASSOCIATED PRESS (Mar. 19, 2019), https://www.apnews.com/38c0dbd8acb14e3fbc7911ea18fafd58; Julia Angwin & Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA (Oct. 28, 2016), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.
Discriminatory Delivery: Levi Kaplan et al., *Measurement and Analysis of Implied Identity in Ad Delivery Optimization*, In *Proc. 22nd ACM Internet Measurement Conf.*, ASS'N FOR COMPUTING MACH. (Oct. 2022), https://dl.acm.org/doi/pdf/10.1145/3517745.3561450; Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, 3 PROC. ACM ON HUMAN-COMPUTER INTERACTION, No. 199 (Nov. 2019), https://dl.acm.org/doi/10.1145/3359301; Ava Kofman & Ariana Tobin, *Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement*, PROPUBLICA (Dec. 13, 2019), https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement; Louise Matsakis, *Facebook's Ad System Might be Hard-Coded for Discrimination*, WIRED (Apr. 6, 2019), https://www.wired.com/story/facebooks-ad-system-discrimination/.

[7] Laura W. Murphy & Megan Cacace, *Facebook's Civil Rights Audit – Final Report*, FACEBOOK 72–82 (July 8, 2020), https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf.

[8] Tracy Jan & Elizabeth Dwoskin, *HUD is Reviewing Twitter's and Google's Ad Practices as Part of Housing Discrimination Probe*, WASH. POST (Mar. 28, 2019), https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/.

[9] Douglas MacMillian, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, WASH. POST (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.

- Landlords and other housing providers use social media targeted advertising tools to engage in discrimination on the basis of race, sex, and age.[10]

- Landlords use tenant screening and background check algorithmic systems that frequently produce flawed reports that cause denials of lease applications.[11] These oversimplified recommendation systems disproportionately impact Black and Latino tenants, making it harder for them to secure affordable housing.[12] The DOJ has said that tenant screening and risk scoring algorithms are subject to the Fair Housing Act.[13] More recently, four prospective tenants sued a Jacksonville real estate company alleging that the company's use of a tenant screening tool disproportionately rejected Black applicants.[14]

- Online real estate brokerage Redfin was sued for engaging in redlining in violation of the Fair Housing Act. Redfin offered limited service to homes under a certain price, which depressed sale prices. The National Fair Housing Alliance found this policy varied in different cities and had a racially disparate impact, discriminating against buyers and sellers of homes in communities of color.[15]

- Some of the largest property managers in the country use property management software company RealPage's rent-setting algorithm. The algorithm allegedly

[10] *See* Brief of the American Civil Liberties Union Foundation, the Lawyers' Committee for Civil Rights Under Law, the National Fair Housing Alliance, and the Washington Lawyers' Committee for Civil Rights and Urban Affairs, as *Amici Curiae* Supporting Appellant and Reversal, *Opiotennione v. Bozzuto Mgmt. Co.*, No. 21-1919, (4th Cir. 2021), ECF No. 49-2, https://www.lawyerscommittee.org/wp-content/uploads/2022/08/3.-Opiotennione-v.-Bozzuto-Mgmt-Corp-amicus-brief.pdf.

[11] *See* Lauren Kirchner & Matthew Goldstein, *Access Denied: Faulty Automated Background Checks Freeze Out Renters*, THE MARKUP & N.Y. TIMES (May 28, 2020), https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters.

[12] *See* Kaveh Waddell, *How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times*, CONSUMER REPS. (Mar. 11, 2021), https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/.

[13] *See* Statement of Interest of the United States at 12–15, *Louis v. SafeRent Solutions, LLC*, No. 22-cv-10800 (Jan. 09, 2023), ECF No. 37; Khari Johnson, *Algorithms Allegedly Penalized Black Renters. The US Government is Watching*, WIRED (Jan. 16, 2023), https://www.wired.com/story/algorithms-allegedly-penalized-black-renters-the-us-government-is-watching/.

[14] Anne Maxwell, *Lawsuit Accuses Jacksonville Real Estate Company of Racial Discrimination in Tenant Screening Process*, NEWS4JAX (Oct. 26, 2023), https://www.news4jax.com/news/local/2023/10/26/lawsuit-accuses-jacksonville-real-estate-company-of-racial-discrimination-in-tenant-screening-process/.

[15] Associated Press, *Redfin to Pay $4 Million to Settle Lawsuit Alleging Housing Discrimination*, MARKETWATCH (May 2, 2022), https://www.marketwatch.com/story/redfin-to-pay-4-million-to-settle-lawsuit-alleging-housing-discrimination-01651500520.

draws on private data, including the rent prices that local competitors charge, to inflate prices and stifle market competition through its rent recommendations.[16]

- Online vacation rental marketplace Airbnb enabled landlords to reject prospective guests with what were perceived to be distinctly Black names at higher rates than guests with what were perceived to be distinctly white names.[17]

- A scoring system used to determine priority for subsidized housing by the Los Angeles Homeless Services Authority and other jurisdictions across the United States discriminated against Black and Latino people experiencing homelessness in Los Angeles. In 2021, for people experiencing homelessness in Los Angeles who were under age 25, the survey-based system gave 67% of white people top priority, compared to only 46% of Black people and 56% of Latino people. The disparity occurred despite Black people being overrepresented in Los Angeles County's population of people experiencing homelessness.[18]

B. Employment

- A major report from Upturn found that algorithms used to automate parts of the hiring process can produce discriminatory outcomes. Predictive hiring tools play "a powerful role in determining who learns of open positions" but can "reproduce patterns of inequity at all stages of the hiring process, even when tools explicitly ignore race, gender, age, and other protected attributes."[19]

- Automated tools—including those using facial recognition or facial analysis—are increasingly a prevalent and pervasive part of the hiring process, but there are

[16] Heather Vogell et al., *Rent Going Up? One Company's Algorithm Could be Why*, PROPUBLICA (Oct. 15, 2022), https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent; Heather Vogell, *Senators Had Questions for the Maker of a Rent-Setting Algorithm. The Answers were "Alarming."*, PROPUBLICA (Mar. 21, 2023), https://www.propublica.org/article/yieldstar-rent-increase-realpage-warren-sanders.

[17] Benjamin Edelman et al., *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, AM. ECON. J.: 9 APPLIED ECON. 1, 1–22 (Apr. 2017), https://www.aeaweb.org/articles?id=10.1257/app.20160213; *see also* Sara Clemence, *Black Travelers Say Home-Share Hosts Discriminate, and a New Airbnb Report Agrees*, N.Y. TIMES (Dec. 18, 2022), https://www.nytimes.com/2022/12/13/travel/vacation-rentals-racism.html.

[18] Colin Lecher & Maddy Venrer, *Black and Latino Homeless People Rank Lower on L A.'s Housing Priority List*, L.A. TIMES & THE MARKUP (Feb. 28, 2023), https://www.latimes.com/california/story/2023-02-28/black-latino-homeless-people-housing-priority-list-los-angeles.

[19] Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN 1 (Dec. 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.

serious concerns that these systems are racially biased and there is little transparency to verify their safety or efficacy.[20] Some companies are now using large language models, such as ChatGPT, to assess resumes. However, an analysis of equally-qualified resumes found that ChatGPT demonstrated racial bias based on the name of an applicant.[21]

- In August 2023, the Equal Employment Opportunity Commission ("EEOC") filed a joint notice of settlement with the iTutor Group, settling claims by the EEOC that the company used an algorithmic screening tool that automatically rejected women applicants over 55 and male applicants over 60.[22] Under the terms of the agreement, the company agreed to $365,000 to applicants who were automatically rejected due to their age.[23] This marks the EEOC's first settlement of an alleged algorithmic discrimination lawsuit.

- Facebook's targeted advertising systems described above in relation to housing also discriminate in employment. Employment ads online can discriminate in both their targeting and in their algorithmic delivery.[24]

- Amazon previously used a machine learning tool to assess job applicants for technical positions, but it systematically discriminated in favor of men.[25]

- Algorithms are becoming more common tools to aid human resources departments for recruitment and development, but there are concerns that these tools can

[20] *See* Avi Asher-Schapiro, *AI is Taking Over Job Hiring, But Can It be Racist?*, REUTERS (June 7, 2021), https://www.reuters.com/article/global-tech-ai-hiring/analysis-ai-is-taking-over-job-hiring-but-can-it-be-racist-idUSL5N2NF5ZC.

[21] Leon Yin et al., *OpenAI's GPT is a Recruiter's Dream Tool. Tests Show There's Racial Bias*, BLOOMBERG (Mar. 7, 2024), https://www.bloomberg.com/graphics/2024-openai-gpt-hiring-racial-discrimination/.

[22] Press Release, Equal Emp. Opportunity Comm'n, iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit (Sept. 11, 2023), https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit.

[23] *Id.*

[24] *See, e.g.*, Rory Cellan-Jones, *Facebook Accused of Allowing Sexist Job Advertising*, BBC (Sept. 9, 2021), https://www.bbc.com/news/technology-58487026; Jeff Horwitz, *Facebook Algorithm Shows Gender Bias in Job Ads, Study Finds*, WALL ST. J. (Apr. 9, 2021), https://www.wsj.com/articles/facebook-shows-men-and-women-different-job-ads-study-finds-11617969600; Nicolas Kayser-Bril, *Automated Discrimination: Facebook Uses Gross Stereotypes to Optimize Ad Delivery*, ALGORITHM WATCH (Oct. 18, 2020), https://algorithmwatch.org/en/automated-discrimination-facebook-google/.

[25] Jeffrey Dastin, *Insight - Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insightidUSKCN1MK08G.

contribute to discrimination.[26] These "bossware" tools are being sold to government agencies as well.[27]

- Employee surveillance tools deployed during the pandemic to monitor remote workers are very invasive and likely to persist beyond the pandemic.[28] These tools disparately impact workers of color, such as Black workers who "routinely struggled to be recognized by the face-scanning systems in a way that their lighter-skinned colleagues did not."[29]
- Digital identity credentialling services like ID.me, which also uses facial recognition technology, have created barriers to access to unemployment benefits and other government benefits, particularly by "low-income people, the elderly, immigrants and other disadvantaged groups."[30]
- A pregnancy-tracking app offered access to user data to employers who bought the app for their workers, as well as to health insurers, raising fears of pregnancy discrimination and other intrusions.[31]

C. Credit and Finance

- Some debt collectors are now using AI chatbots, like ChatGPT, to contact and recover funds from debtors. However, the use of these tools may exacerbate existing racial disparities in debt collection and enforcement by targeting Black people and other people of color at higher rates.[32]

[26] *See* Alina Köchling & Marius Claus Wehner, *Discriminated by An Algorithm: A Systematic Review of Discrimination and Fairness by Algorithmic Decisionmaking in the Context of HR Recruitment and HR Development*, 13 BUS. RSCH. 795 (2020), https://doi.org/10.1007/s40685-020-00134-w.

[27] Maddy Varner, *Public Agencies Are Buying Up AI-Driven Hiring Tools and "Bossware"*, THE MARKUP (Dec. 23, 2021), https://themarkup.org/news/2021/12/23/public-agencies-are-buying-up-ai-driven-hiring-tools-and-bossware.

[28] *See* Danielle Abril & Drew Harwell, *Keystroke Tracking, Screenshots, and Facial Recognition: The Boss May Be Watching Long After the Pandemic Ends*, WASH. POST (Sept. 24, 2021), https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/.

[29] *Id.*

[30] CMTY. LEGAL SERVS. OF PHILA., *ID.me Presents Barriers to Unemployment Insurance and Other Government Benefits* (Nov. 3, 2021), https://clsphila.org/employment/id-me-paper/.

[31] 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/.

[32] Corin Faife, *Debt Collectors Want to Use AI Chatbots to Hustle People for Money*, VICE : MOTHERBOARD (May 18, 2023), https://www.vice.com/en/article/bvjmm5/debt-collectors-want-to-use-ai-chatbots-to-hustle-people-for-money.

- One study found that FinTech algorithms charge otherwise equivalent Black and Latino borrowers higher rates—5.3 basis points higher for purchase mortgages and 2.0 basis points higher for refinance mortgages. While FinTech lenders are less discriminatory than face-to-face lending, algorithmic lending is still discriminatory.[33]

- Another study similarly found that biases in "algorithmic strategic pricing" resulted in Black and Latino borrowers paying higher interest rates on home purchase and refinance loans, amounting to $250–$500 million annually.[34]

- In 2020, at a time of historically low interest rates and an opportunity to lock in the ability to build long-term home equity, Wells Fargo's algorithms racially discriminated in mortgage refinancing, rejecting over half of Black applicants, while approving over 70% of white applicants.[35]

- More recently, reporters found that Navy Federal Credit Union approved white applicants by a nearly 29-point gap higher than Black applicants. This disparity is so significant that the bank approved white applicants making less than $62,000 at a higher rate than Black applicants making $140,000 or more.[36]

- Lax data security at credit reporting agencies such as Experian[37] and Equifax[38] have resulted in breaches exposing the sensitive credit data of millions of Americans. As the FTC has found, identity theft and fraud disproportionately

[33] *See* Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era* (Nat'l Bureau Econ. Rsch. Working Paper No. 25943, 2019), https://www.nber.org/system/files/working_papers/w25943/w25943.pdf.

[34] Laura Counts, *Minority Homebuyers Face Widespread Statistical Lending Discrimination, Study Finds*, U.C. BERKELEY HAAS SCH. OF BUS. (Nov. 13, 2018), https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/.

[35] Shawn Donnan et al., *Wells Fargo Rejected Half Its Black Applicants in Mortgage Refinancing Boom*, BLOOMBERG (Mar. 11, 2022), https://www.bloomberg.com/graphics/2022-wells-fargo-black-home-loan-refinancing; *see also* Emily Flitter, *A Black Homeowner is Suing Wells Fargo, Claiming Discrimination*, N.Y. TIMES (Mar. 21, 2022), https://www.nytimes.com/2022/03/21/business/wells-fargo-mortgages-discrimination-suit.html.

[36] Casey Tolan et al., *The Nation's Largest Credit Union Rejected More than Half Its Black Conventional Mortgage Applicants*, CNN (Dec. 14, 2023), https://edition.cnn.com/2023/12/14/business/navy-federal-credit-union-black-applicants-invs/index.html.

[37] KREBS ON SEC., *Experian API Exposed Credit Scores of Most Americans* (Apr. 28, 2021), https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/.

[38] *See Equifax, Inc.*, FTC File No. 172 3203 (July 23, 2019), No. 1:19-cv-03297-TWT (N.D. Ga.), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc.

impact communities of color and low-income consumers are also less likely to have the resources to bounce back after experiencing fraud.[39]

- Google's search engine has served users ads for payday loans when they ran searches for terms associated with financial distress, such as "[I] need money to pay my rent."[40]

- The same discrimination issues in Facebook's advertising system discussed above with regard to the targeting and delivery of housing and employment ads also apply to credit ads.[41] After reporters discovered that Facebook targeted ads for financial services based on age, the company pledged to remove the discriminatory content.[42]

- Data used to score consumers' credit has been shown to be capable of predicting the race and gender of loan applicants.[43]

- Algorithms used to approve or deny loans discriminate even when sensitive data like race or gender are not collected. A study of one global fintech lender found that proxy data correctly predicted gender 91% of the time and led a machine

[39] *See* FTC, SERVING COMMUNITIES OF COLOR: A STAFF REPORT ON THE FEDERAL TRADE COMMISSION'S EFFORTS TO ADDRESS FRAUD AND CONSUMER ISSUES AFFECTING COMMUNITIES OF COLOR (2021) [hereinafter SERVING COMMUNITIES OF COLOR], https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf; *see also* Sarah Dranoff, *Identity Theft: A Low-Income Issue*, AM. BAR ASS'N (Dec. 15, 2014), https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/.

[40] Aaron Reike & Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, UPTURN 15 (Oct. 2015), https://www.upturn.org/reports/2015/led-astray/.

[41] *See, e.g.*, Joel Rosenblatt, *Facebook Financial-Services Ads Accused of Male Bias in Suit*, BLOOMBERG (Oct. 31, 2019), https://www.bloomberg.com/news/articles/2019-10-31/facebook-financial-services-ads-accused-of-male-bias-in-lawsuit; Corin Faife & Alfred Ng, *Credit Card Ads Were Targeted by Age, Violating Facebook's Anti-Discrimination Policy*, THE MARKUP (Apr. 29, 2021), https://themarkup.org/citizen-browser/2021/04/29/credit-card-ads-were-targeted-by-age-violating-facebooks-anti-discrimination-policy.

[42] Corin Faife & Alfred Ng, *Facebook Pledges to Remove Discriminatory Credit and Loan Ads Discovered by The Markup*, THE MARKUP (May 4, 2021), https://themarkup.org/citizen-browser/2021/05/04/facebook-pledges-to-remove-discriminatory-credit-and-loan-ads-discovered-by-the-markup.

[43] *See* Bertrand K. Hassani, *Societal Bias Reinforcement Through Machine Learning: A Credit Scoring Perspective*, 1 AI & ETHICS 239 (2020), https://link.springer.com/article/10.1007/s43681-020-00026-z.

learning algorithm to overestimate women applicants' default rate. Including gender data reduced the algorithm's gender discrimination by 2.8 times.[44]

D. Insurance

- Health insurance companies buy information from data brokers to predict costs of patient health care, including demographic and lifestyle data, which can result in higher rates for consumers of color. As an insurance salesman joked, "God forbid you live on the wrong street these days . . . You're going to get lumped in with a lot of bad things."[45] All forms of insurance are now "adjusting premiums and policies based on new forms of surveillance."[46]

- A common algorithm designed to reduce the overutilization of emergency medical services by children can lead insurance companies to charge Black and Hispanic patients more than white patients. This occurs because Black and Hispanic children are significantly more likely to have emergency visits classified as "nonemergent," forcing families of color to pay higher rates for needed care.[47]Analyses of car insurance premiums in various states have shown that Black and Brown neighborhoods are systematically charged higher premiums than white neighborhoods of similar risk, regardless of neighborhood affluence.[48] Insurance premiums are set by actuarial algorithms using many non-driving factors, which contributes to higher rates in Black neighborhoods and for

[44] Stephanie Kelley et al., *Removing Demographic Data Can Make AI Discrimination Worse*, HARV. BUS. REV. (Mar. 6, 2023), https://hbr.org/2023/03/removing-demographic-data-can-make-ai-discrimination-worse; Stephanie Kelley et al., *Antidiscrimination Laws, Artificial Intelligence, and Gender Bias: A Case Study in Nonmortgage Fintech Lending*, 24 MFG. & SERV. OPERATIONS MGMT. 3039 (2022), https://pubsonline.informs.org/doi/epdf/10.1287/msom.2022.1108.

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

[46] Sarah Jeong, *Insurers Want to Know How Many Steps You Took Today*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/2019/04/10/opinion/insurance-ai.html; *see also* Angela Chen, *Why the Future of Life Insurance May Depend on Your Online Presence*, THE VERGE (Feb. 7, 2019), https://www.theverge.com/2019/2/7/18211890/social-media-life-insurance-new-york-algorithms-big-data-discrimination-online-records.

[47] Frank Diamond, *Algorithm Used to Cut ER Overutilization for Kids Penalizes Black, Hispanic Patients: Study*, FIERCE HEALTHCARE (May 10, 2023), https://www.fiercehealthcare.com/payers/method-used-cut-emergency-department-overutilization-kids-penalizes-blacks-hispanics-study.

[48] Julia Angwin et al., *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, PROPUBLICA (Apr. 5, 2017), https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk.

individuals with less education or lower-paying jobs.[49] These scoring algorithms judge applicants "less on driving habits and increasingly on socioeconomic factors."[50]

- Allstate attempted to use a personalized pricing algorithm in Prince George's County, Maryland, which the state rejected as discriminatory. The algorithm would have charged consumers more if they were unlikely to switch to another car insurance company,[51] contributing to discriminatory higher premiums routinely paid by consumers of color who often lack competitive options for insurance. The Allstate personalized pricing algorithm was still implemented in other states.[52]

- Car insurance companies collect a wide array of detailed data from cars—including not just vehicle performance and location data, but also driver habits and characteristics such as driver name, driver fatigue, driver heartrate, and the language used on a dashboard display.[53] Companies use this data in usage-based insurance, which charges higher premiums to "risky drivers."[54] These types of

[49] *See* Douglass Heller, *Auto Insurance: A National Issue of Economic Justice*, CONSUMER FED'N OF AM. (Jan. 2019), https://consumerfed.org/wp-content/uploads/2020/01/Summary-of-Auto-Insurance-Research.pdf; Kaveh Waddell, *Why Your Education and Job Could Mean You're Paying Too Much for Car Insurance*, CONSUMER REPS. (Jan. 28, 2021), https://www.consumerreports.org/car-insurance/why-your-education-and-job-could-mean-youre-paying-too-much-for-car-insurance-a3116553820/.

[50] CONSUMER REPS., *The Truth About Car Insurance* (July 30, 2015), https://www.consumerreports.org/cro/car-insurance/auto-insurance-special-report/index.htm.

[51] Maddy Varner & Aaron Sankin, *Suckers List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders*, THE MARKUP & CONSUMER REPS. (Feb. 25, 2020), https://themarkup.org/allstates-algorithm/2020/02/25/car-insurance-suckers-list.

[52] *See* Aaron Sankin, *Michigan Regulators Question Allstate's Car Insurance Pricing*, THE MARKUP & CONSUMER REPS. (Feb. 9, 2021), https://themarkup.org/allstates-algorithm/2021/02/09/michigan-regulators-question-allstates-car-insurance-pricing; Aaron Sankin, *Newly Public Documents Allege Allstate Overcharged Loyal California Customers $1 Billion,* THE MARKUP (Feb. 1, 2022), https://themarkup.org/allstates-algorithm/2022/02/01/newly-public-documents-allege-allstate-overcharged-loyal-california-customers-1-billion.

[53] Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies*, N.Y. TIMES (Mar. 13, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html; Jon Keegan & Alfred Ng, *Who is Collecting Data from Your Car?*, THE MARKUP (July 27, 2022), https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car; *see also, e.g.*, HIGH MOBILITY, Airtable, *Auto API Level 13*, https://www.high-mobility.com/car-data/overview (click an item in the menu and then click "Open Airtable" to see the Full Data Catalog for that item); Jen Caltrider et al., *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, MOZILLA FOUND.: *PRIVACY NOT INCLUDED (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[54] Keegan & Ng, *supra* note 53.

data collection systems provide the raw materials that may fuel discriminatory pricing algorithms, as discussed above.

- Insurers seek to collect data from fitness trackers about the health and wellness habits of their customers.[55] To the extent these devices are luxury items unavailable to low-income consumers, the datasets built from them could be skewed. This health data will reaffirm a "normal" based on more affluent and whiter consumers. Low-income consumers could end up paying higher insurance rates if they are unable to afford the tracking devices, penalizing their poverty.

E. Public health and healthcare

- Social media news feed algorithms and advertising systems significantly contributed to the amplification of health disinformation about COVID-19.[56] In the first months of the pandemic, "[c]ontent from the top 10 websites spreading health misinformation had almost four times as many estimated views on Facebook as equivalent content from the websites of 10 leading health institutions, such as the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC)."[57] Public health agencies have faced particular difficulties getting their paid public service announcements to reach Black social media users.[58] This disparity in reach has real-life consequences, as COVID disproportionately harms Black and Hispanic Americans, who experience higher disease prevalence, hospitalization, and mortality compared to whites and who have less access to healthcare as a consequence of systemic racism.[59]

[55] Christopher Ingraham, *An Insurance Company Wants You to Hand Over Your Fitbit Data So It Can Make More Money. Should You?*, WASH. POST (Sept. 25, 2018), https://www.washingtonpost.com/business/2018/09/25/an-insurance-company-wants-you-hand-over-your-fitbit-data-so-they-can-make-more-money-should-you/.

[56] *See* Virginia Alvino Young, *Nearly Half of the Twitter Accounts Discussing 'Reopening America' May Be Bots*, CARNEGIE MELLON UNIV. (May 27, 2020), https://www.cmu.edu/news/stories/archives/2020/may/twitter-bot-campaign.html; Ryan Gallagher & Mark Bergen, *Google Helps Place Ads on Sites Amplifying Covid-19 Conspiracies*, BLOOMBERG (June 1, 2020), https://www.bloomberg.com/news/articles/2020-06-01/google-helps-place-ads-on-sites-amplifying-covid-19-conspiracies.

[57] AVAAZ, *Facebook's Algorithm: A Major Threat to Public Health* (Aug. 19, 2020), https://secure.avaaz.org/campaign/en/facebook_threat_health/.

[58] *See* Corin Faife & Dara Kerr, *Official Information About COVID-19 Is Reaching Fewer Black People on Facebook*, THE MARKUP (Mar. 4, 2021), https://themarkup.org/citizen-browser/2021/03/04/official-information-about-covid-19-is-reaching-fewer-black-people-on-facebook.

[59] *See, e.g.*, William Mude et al., *Racial Disparities in COVID-19 Pandemic Cases, Hospitalizations, and Deaths: A Systematic Review and Meta-analysis*, 11 J. GLOB. HEALTH (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8248751/.

- Facebook's internal communications indicate that the company was well aware of the growing threat of COVID-19 misinformation and its broader societal impact. "Facebook made a conscious decision to continue hosting vaccine misinformation rather than aggressively purge it."[60]

- Several widely used algorithms for identifying health needs of patients have been shown to be racially biased. By predicting health costs rather than illness, combined with unequal access to healthcare, the algorithm underpredicts sickness in Black patients and limits access to care.[61] Another algorithm made "wildly irrational" decisions depriving necessary care to people with disabilities.[62] More recently, researchers found that an algorithm commonly used to evaluate kidney transplant patients overestimated the kidney function of Black patients, disproportionately delaying transplants for Black patients despite their higher risk.[63]

- Even when deployed to remedy existing human biases within healthcare, algorithmic tools can nonetheless perpetuate these biases and inaccuracies because of their training data. For instance, a recent study found that the use of algorithmic diagnostic tools for assessing skin diseases *increased* the gap between the accurate diagnoses for patients with light skin tones compared to patients with darker skin tones.[64]

- Social media platforms, particularly Instagram, push content to teenage girls that is known to be harmful to their physical and mental health, because it maximizes

[60] Dell Cameron & Mack DeGeurin, *How Meta Became the Internet's Biggest Hub of Covid-19 Misinformation*, GIZMODO (Oct. 20, 2022), https://gizmodo.com/facebook-papers-covid-19-coronavirus-misinformation-1849667132.

[61] Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCI. 447 (2019), https://www.science.org/doi/10.1126/science.aax2342; *see also* Trishan Panch et al., *Artificial Intelligence and Algorithmic Bias: Implications for Health Systems*, 9 J. GLOB. HEALTH (2019) (offering definitions of algorithmic bias in health systems), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6875681/.

[62] Erin McCormick, *What Happened When a 'Wildly Irrational' Algorithm Made Crucial Healthcare Decisions*, THE GUARDIAN (July 2, 2021), https://www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions.

[63] Lauran Neergard, *A Biased Test Kept Thousands of Black People from Getting a Kidney Transplant. It's Finally Changing*, AP NEWS (Apr. 1, 2024), https://apnews.com/article/kidney-transplant-race-black-inequity-bias-d4fabf2f3a47aab2fe8e18b2a5432135.

[64] Shanice Harris, *Racial Bias Exists in Photo-based Medical Diagnosis Despite AI Help*, NW. UNIV.: NW. NOW (Feb. 5, 2024), https://news.northwestern.edu/stories/2024/02/new-study-suggests-racial-bias-exists-in-photo-based-diagnosis-despite-assistance-from-fair-ai/.

user engagement.[65] Internal company research observed, "'Thirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse. . . . Teens blame Instagram for increases in the rate of anxiety and depression.'"[66] Over-sexualization of girls on social media can be particularly detrimental to the mental health of Black girls, whose bodies are subjected to more critiques.[67] When teens engaged in suicidal ideation, 6% of them traced it to Instagram.[68] Like Instagram, research shows that TikTok pushes harmful content to some teenagers. Researchers who set up accounts pretending to be 13-year-old teenagers found that TikTok recommended suicide and eating disorder content within minutes once the accounts viewed and liked content related to body image, eating disorders, and mental health.[69]

- When users searched Google for abortion care, the search engine often steered the users instead to "crisis pregnancy centers that do not provide abortions and sometimes actively try to dissuade people from getting them."[70] People of color are less likely to have access to specialty medical care,[71] and therefore are more likely to turn to the internet to find healthcare.

- Data broker SafeGraph collected, packaged, and sold location data specifically tracking visitors to over 600 Planned Parenthood locations.[72] There is significant concern that data collected by Google and other entities, especially location data,

[65] *See* Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, Wall St. J. (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

[66] *Id.*; *see also* 60 Minutes Overtime, *Facebook Knew Instagram Was Pushing Girls to Dangerous Content: Internal Document*, CBS News (Dec. 11, 2022), https://www.cbsnews.com/news/facebook-instagram-dangerous-content-60-minutes-2022-12-11/.

[67] Wells et al., *supra* note 65.

[68] *Id.*

[69] CTR. FOR COUNTERING DIGIT. HATE, *Deadly by Design: TikTok Pushes Harmful Content Promoting Eating Disorders and Self-Harm into Users' Feeds* 7, 10, 19 (Dec. 2022), https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf.

[70] Gerrit De Vynck, *Google Maps Will Label Clinics That Provide Abortion Services*, N.Y. TIMES (Aug. 25, 2022), https://www.washingtonpost.com/technology/2022/08/25/google-maps-abortions/.

[71] *See* Christopher Cai et al., *Racial and Ethnic Disparities in Outpatient Visit Rates Across 29 Specialties*, 181 J. AM. MED. ASS'N. 1525-27 (July 19, 2021), https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2782019 ("Racial/ethnic minority groups are more likely to reside in areas with a shortage of physicians and less likely to receive specialty referrals from primary care physicians.").

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

could be used to prosecute people seeking reproductive healthcare.[73] Access to reproductive healthcare is essential for Black women and low-income women, who experience higher rates of unintended pregnancy and are more likely to have abortions.[74] Consequently, surveillance of people seeking reproductive healthcare is likely to disproportionately impact these populations.

- Despite Google's pledge after the overturning of *Roe v. Wade* to delete location data for visits to abortion clinics,[75] testing showed that searches for directions and routes taken to abortion clinics, and other data, like abortion-related search engine history, can remain visible on users' activity pages for months after being logged.[76] Google has a notable history of collecting location data against users' wishes.[77]
- Facebook gave Nebraska law enforcement, in response to a court order, the private communications of a teenager who sought medication for an at-home abortion.[78] Facebook has collected sensitive patient information from healthcare and hospital websites, including data on people seeking abortions and children.[79] It collected

[73] *See* Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, POLITICO (July 18, 2022), https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906.

[74] *See* Katherine Kortsmit et al., Ctrs. For Disease Control & Prevention, *Abortion Surveillance – United States, 2018*, 69 MORBIDITY & MORTALITY WEEKLY REP. SURVEILLANCE SUMMARIES 6 (2020), https://www.cdc.gov/mmwr/volumes/69/ss/pdfs/ss6907a1-H.pdf; Jenna Jerman et al., *Characteristics of U.S. Abortion Patients in 2014 and Changes Since 2008*, GUTTMACHER INST. 11 (2016), https://www.guttmacher.org/sites/default/files/report_pdf/characteristics-us-abortion-patients-2014.pdf.

[75] *See* Jen Fitzpatrick, *Protecting People's Privacy on Health Topics*, GOOGLE: THE KEYWORD (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/.

[76] Johana Bhuiyan, *Googling Abortion? Your Details Aren't as Private as You Think*, THE GUARDIAN (Nov. 29, 2022), https://www.theguardian.com/world/2022/nov/29/abortion-rights-us-google-roe-dobbs; Geoffrey A. Fowler, *Google Promised to Delete Sensitive Data. It Logged My Abortion Clinic Visit*, WASH. POST (May 9, 2023), https://www.washingtonpost.com/technology/2023/05/09/google-privacy-abortion-data/.

[77] *See* Dave Collins & Marcy Gordon, *40 States Settle Google Location-Tracking Charges for $392M*, ASSOCIATED PRESS (Nov. 14, 2023), https://apnews.com/article/google-privacy-settlement-location-data-57da4f0d3ae5d69b14f4b284dd084cca.

[78] Jason Koebler & Anna Merlan, *This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion*, VICE: MOTHERBOARD (Aug. 9, 2022), https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion.

[79] *See* Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (June 5, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients; Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook*, THE MARKUP (June 21, 2022), https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook; Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

health information, including ovulation data, from health apps without user consent.[80]

- Health apps often collect sensitive personal data and data that can be used to track people seeking healthcare, including advertising identifiers, email addresses, and location data, and they often share this data with third parties.[81] This information can reveal people seeking abortions, be shared with employers, or sold to insurance companies. This can disproportionately affect women of color and low-income women who are more likely to seek abortion services.

- Several online healthcare companies, including an online therapy platform, a pharmacy, and a period tracking app, have reached settlements in recent years with the FTC following allegations that they shared sensitive user data to third parties to enable targeted advertising.[82]

- Data brokers also sell personal data to health care providers, including "criminal records, online purchasing histories, retail loyalty programs and voter registration data."[83] These data can be fed into algorithms used to classify patients' health risks and can produce biases if not handled correctly.[84] Similarly, hospitals deidentify data so that they can share or sell them to researchers and private companies, but there are concerns about the adequacy of the deidentification, raising similar risks.[85]

- Poorly designed medical research can lead to procedures or technologies that misdiagnose patients. One study noted that neural networks used to analyze and classify skin lesions are often trained on samples of predominantly white patients,

[80] Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[81] Gioacchino Tangari et al., *Mobile Health and Privacy: Cross Sectional Study*, BMJ (June 17, 2021), https://www.bmj.com/content/373/bmj.n1248.

[82] Josh Sisco & Ruth Reader, *FTC Reaches Deal With Online Company Over Data Misuse Claims*, POLITICO (Mar. 2, 2023), https://www.politico.com/news/2023/03/02/ftc-data-misuse-betterhelp-00085182.

[83] Mohana Ravindranath, *Does Your Doctor Need to Know What You Buy on Amazon?*, POLITICO (Oct. 30, 2018), https://www.politico.com/story/2018/10/30/the-doctor-will-see-through-you-now-893437.

[84] *See* Obermeyer, *supra* note 61.

[85] Nicole Wetsman, *Hospitals Are Selling Treasure Troves of Medical Data – What Could Go Wrong?*, THE VERGE (June 23, 2021), https://www.theverge.com/2021/6/23/22547397/medical-records-health-data-hospitals-research; *see also* Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, SCI. AM. (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/;

and thus are only half as accurate when diagnosing Black patients.[86] Similarly, health insurers increasingly rely on machine learning models to predict everything from disease onset to likelihood of hospitalization and medication adherence, which can give rise to bias.[87]

F. Education

- Online and for-profit colleges specifically target Black and Latino prospective students with predatory marketing practices while providing low-quality education and high debt loans.[88]

- Algorithms used to determine admission to New York City high schools "regularly screened out" Black and Latino students from the city's top performing schools, consistently admitting them at lower rates than white or Asian students.[89]

- Higher education institutions are increasingly adopting "student success analytics" intended to aid students in their studies.[90] Universities have used race as a "high impact predictor" in risk assessment software used to predict which students are likely to succeed or drop out, raising concerns that Black students

[86] Natalia Norori et al., *Addressing Bias in Big Data and AI for Health Care: A Call for Open Science*, 2 PATTERNS (2021), https://doi.org/10.1016/j.patter.2021.100347.

[87] *See* Stephanie S. Gervasi et al., *The Potential for Bias in Machine Learning and Opportunities for Health Insurers to Address It*, 41 HEALTH AFFS. 212 (2022), https://doi.org/10.1377/hlthaff.2021.01287.

[88] Genevieve (Genzie) Bonadies et al., *For-Profit Schools' Predatory Practices and Students of Color: A Mission to Enroll Rather than Educate*, HARV. L. REV. BLOG (July 30, 2018), https://blog.harvardlawreview.org/for-profit-schools-predatory-practices-and-students-of-color-a-mission-to-enroll-rather-than-educate/; *see also* Larry Abramson, *For-Profit Schools Under Fire for Targeting Veterans*, NPR (Apr. 9, 2012), https://www.npr.org/2012/04/09/150148966/for-profit-schools-under-fire-for-targetingveterans.

[89] Colin Lecher & Maddy Varner, *NYC's School Algorithms Cement Segregation. This Data Shows How*, THE MARKUP (May 26, 2021), https://themarkup.org/machine-learning/2021/05/26/nycs-school-algorithms-cement-segregation-this-data-shows-how.

[90] Maureen Guarcello et al., *Discrimination in a Sea of Data: Exploring the Ethical Implications of Student Success Analytics*, EDUCAUSE REV. (Aug. 24, 2021), https://er.educause.edu/articles/2021/8/discrimination-in-a-sea-of-data-exploring-the-ethical-implications-of-student-success-analytics.

will be steered away from pursuing math and science.[91] Black students were deemed “higher risk for failure” as much as four times as often as white peers.[92]

- Colleges and universities often use algorithms to allocate scholarships, but these tools can exacerbate low graduation rates, high student debt, and racial inequality in access to higher education.[93] Enrollment algorithms often discriminate against people of color and women.[94] Relatedly, some universities install tracking software on their school websites to collect data on “test scores, ZIP codes, high school transcripts, academic interests, Web browsing histories, ethnic backgrounds and household incomes” to create predictive scores of how likely students are to enroll if admitted.[95] More than 75 percent of colleges and universities use analytics in enrollment management and admissions decisions.[96]

- Naviance college admissions software, used by approximately two-thirds of high schoolers, allows colleges to target ads to prospective students on the basis of race and location. An investigation found examples of some universities, including the University of Kansas, University of Southern Maine, and University of Massachusetts Boston, deliberately—sometimes exclusively—advertising to white students.[97]

[91] Todd Feathers, *Major Universities Are Using Race as a “High Impact Predictor” of Student Success*, THE MARKUP (Mar. 2, 2021), https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success.

[92] *Id.*; *see also* Todd Feathers, *False Alarm: How Wisconsin Uses Race and Income to Label Students “High Risk”*, THE MARKUP (May 11, 2023), https://themarkup.org/machine-learning/2023/04/27/false-alarm-how-wisconsin-uses-race-and-income-to-label-students-high-risk (example of similar algorithmic bias in secondary education).

[93] Alex Engler, *Enrollment Algorithms Are Contributing to the Crises of Higher Education*, BROOKINGS (Sept. 14, 2021), https://www.brookings.edu/research/enrollment-algorithms-are-contributing-to-the-crises-of-higher-education/.

[94] *See id.*

[95] Douglas MacMillan & Nick Anderson, *Student Tracking, Secret Scores: How College Admissions Offices Rank Prospects Before They Apply*, WASH. POST (Oct. 14, 2019), https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/.

[96] Ronald Yanosky & Pam Arroway, *The Analytics Landscape of Higher Education, 2015*, EDUCAUSE 17 (2015) https://library.educause.edu/~/media/files/library/2015/5/ers1504cl.pdf.

[97] Todd Feathers, *College Prep Software Naviance Is Selling Advertising Access to Millions of Students*, THE MARKUP (Jan. 13, 2022), https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students.

- Surveillance of students disproportionately harms Black and Brown students.[98] These students "rely more heavily on school-issued devices. Therefore, they are subject to more surveillance and . . . interacting with law enforcement, being disciplined, and being outed, than those using personal devices."[99] "Despite assurances and hopes that student activity monitoring will be used to keep students safe, teachers report that it is more frequently used for disciplinary purposes in spite of parent and student concerns."[100]

- A report by Senators Elizabeth Warren and Ed Markey found that "student activity monitoring software may be misused for disciplinary purposes and result in increased contact with law enforcement" and that "[c]ompanies have not taken any steps to determine whether student activity monitoring software disproportionately targets students from marginalized groups" despite evidence that students of color face disparities in discipline.[101] This type of software is being used in Baltimore, for example, where the school district has lent out tens of thousands of laptops to students.[102]

- A facial recognition company marketing school safety technology misled its school district customers about the accuracy of its software, downplaying how frequently it misidentified Black faces and mistakenly flagged objects as weapons.[103] Similarly, "aggression detector" software marketed to schools to monitor students by recording audio and monitoring for "threats" often fail to identify or misidentify

[98] *See* Hannah Quay-de la Vallee & Natasha Duarte, *Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data*, CTR. FOR DEMOCRACY & TECH. (Aug. 2019), https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf; Frida Alim et al., *Spying on Students: School-Issued Devices and Student Privacy*, ELEC. FRONTIER FOUND. (Apr. 15, 2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy.

[99] Elizabeth Laird et al., *Report – Hidden Harms: The Misleading Promise of Monitoring Students Online*, CTR. FOR DEMOCRACY & TECH. (Aug. 3, 2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/.

[100] *Id.*

[101] U.S. Sens. Elizabeth Warren & Ed Markey, *Constant Surveillance: Implications of Around-the-Clock Online Student Activity Monitoring* 3 (Mar. 2022), https://www.warren.senate.gov/imo/media/doc/356670%20Student%20Surveillance.pdf.

[102] Liz Bowie, *Baltimore City Student Laptops Are Monitored for Mentions of Suicide. Sometimes, the Police Are Called.*, BALT. SUN (Oct. 12, 2021), https://www.baltimoresun.com/education/bs-md-laptops-monitoring-20211012-a2j3vsytijhhjj36n57ri5zdhi-story.html.

[103] Todd Feathers, *Facial Recognition Company Lied to School District About its Racist Tech*, VICE: MOTHERBOARD (Dec. 1, 2020), https://www.vice.com/en/article/qjpkmx/fac-recognition-company-lied-to-school-district-about-its-racist-tech.

sounds.[104] Such misidentifications are extremely dangerous to Black children who could be targeted by an armed police response.

- School districts, particularly in metropolitan areas with high numbers of students of color, have bought mobile device forensic tools which allow them to access students' cellphone messages, photos, app data, location data, and other communications.[105] Other schools have used AI-driven software to surveil students' social media for warning signs of violence, without the students' permission or awareness.[106]

- Students of color have reported having difficulties getting remote camera proctoring software, such as Proctorio and ExamSoft, to "see" them regardless of how well-lit their room is. These software tools, which are used to flag potential cheaters, can use facial recognition to track students' actions.[107] Black women, in particular, are at greater risk of being falsely accused of cheating by these automated tools.[108]

G. Public accommodations

- The Social Media Victims Law Center filed a lawsuit against YouTube, Meta, and TikTok, alleging that their content recommendation engines engage in racial profiling and disproportionately push violent, drug-filled, and sexual content to Black youth, including content driving Black kids to engage in self-harm.[109]

[104] 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/.

[105] Tom McKay & Dhruv Mehrotra, *U.S. Schools Are Buying Phone-Hacking Tech That the FBI Uses to Investigate Terrorists*, GIZMODO (Dec. 11, 2020), https://gizmodo.com/u-s-schools-are-buying-phone-hacking-tech-that-the-fbi-1845862393.

[106] *See* Sidney Fussell, *Schools Are Using AI to Check Students' Social Media for Warning Signs of Violence*, GIZMODO (Mar. 22, 2018), https://gizmodo.com/schools-are-using-ai-to-check-students-social-media-for-1824002976.

[107] *See* Anushka Patil & Jonah Engel Bromwich, *How It Feels When Software Watches You Take Tests*, N.Y. TIMES (Sept. 29, 2020), https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html.

[108] *See* Kashmir Hill, *Accused of Cheating by an Algorithm, and a Professor She Had Never Met*, N.Y. TIMES (May 27, 2022), https://www.nytimes.com/2022/05/27/technology/college-students-cheating-software-honorlock.html.

[109] BUSINESSWIRE, *Social Media Victims Law Center Files Suit Against Social Media Giants for the Race-Driven Anguish Suffered by One Small-Town Family* (Aug. 2, 2022), https://www.businesswire.com/news/home/20220802005949/en/Social-Media-Victims-Law-Center-

(footnotes continue on next page)

- Black and Hispanic children who use social media are more likely than not to come across racial harassment—targeting themselves or others—and those exposed are more likely to report symptoms of depression and lower academic self-efficacy.[110]

- Uber enabled drivers to discriminate against passengers with what were perceived to be Black names and provide more expensive services to women passengers.[111]

- Google blocked YouTube advertisers from being able to target ads to "Black Lives Matter" and "Black Power" videos and channels but allowed ad targeting to videos and channels related to "White Lives Matter" and "White Power." Other blocked terms included Black Excellence, LGBTQ, Reparations, Colonialism, Antifascist, American Muslim, Civil Rights, Antiracism, Black is Beautiful, Believe Black Women, Black Trans Lives Matter, I Can't Breathe, Queer, Say Their Names, and more.[112] These blocks undermine the ability to monetize content on these subjects, which in turn affects incentives to produce content on these subjects, and ultimately which content will become popular on the site.

- Google's Keywords Planner ad tool, used to help advertisers choose search terms for their ads, returned pornographic keyword suggestions as its top results in searches for "Black girls," "Latina girls," or "Asian girls." Searching for boys of these races also returned pornographic results. But searches for "white girls" or "white boys" returned no results. "Google's systems contained a racial bias that equated people of color with objectified sexualization while exempting White people from any associations whatsoever. . . . [B]y not offering a significant number of non-pornographic suggestions, this system made it more difficult for

Files-Suit-Against-Social-Media-Giants-for-the-Race-Driven-Anguish-Suffered-by-One-Small-Town-Family; Sharyn Alfonsi, *More than 1,200 Families Suing Social Media Companies Over Kids' Mental Health*, CBS NEWS (Dec. 11, 2022), https://www.cbsnews.com/news/social-media-lawsuit-meta-tiktok-facebook-instagram-60-minutes-2022-12-11/.

[110] Alvin Thomas et al., *Taking the Good with the Bad?: Social Media and Online Racial Discrimination Influences on Psychological and Academic Functioning in Black and Hispanic Youth*, 52 J. YOUTH & ADOLESCENCE 245, 255 (Oct. 2023), https://link.springer.com/article/10.1007/s10964-022-01689-z.

[111] *See* Yanbo Ge et al., *Racial and Gender Discrimination in Transportation Network Companies* (Nat'l Bureau of Econ. Rsch. Working Paper No. 22776, 2016), https://www.nber.org/papers/w22776.

[112] Leon Yin & Aaron Sankin*, Google Blocks Advertisers from Targeting Black Lives Matter YouTube Videos*, THE MARKUP (Apr. 9, 2021), https://themarkup.org/google-the-giant/2021/04/09/google-blocks-advertisers-from-targeting-black-lives-matter-youtube-videos.

marketers attempting to reach young Black, Latinx, and Asian people with products and services relating to other aspects of their lives."[113]

- An algorithm used by Twitter to automatically crop images for tweets systematically cropped out Black faces in favor of white faces, and also exhibited discrimination against Muslims, people with disabilities, and the elderly.[114]

- "Dark patterns" that deceptively trick website and app users to make choices against their self-interest are particularly predatory toward low-income users, people for whom English is a second language, people from nondominant cultures, and people with less digital literacy.[115]

- Automated content moderation systems frequently over-police Black users compared to white users. Internal data showed that Black Instagram users were about 50% more likely to have their accounts automatically disabled than white users. After Facebook executives received those data, they halted further research into racial bias in the system.[116]

- Online stores can use data about where and how a user accesses their site—including geographic location, which can be a proxy for race—to engage in price discrimination.[117] For example, algorithms that distribute discount-related ads tend to direct those ads toward high-income white users.[118]

- A recent analysis of over 700 individuals' data found that, on average, participants had their data shared with Facebook, now known as Meta, by 2,230 companies.

[113] Leon Yin & Aaron Sankin, *Google Ad Portal Equated "Black Girls" with Porn*, THE MARKUP (July 23, 2020), https://themarkup.org/google-the-giant/2020/07/23/google-advertising-keywords-black-girls.

[114] *See* Kevin Collier, *Twitter's Racist Algorithm Is Also Ageist, Ableist and Islamaphobic, Researchers Find*, NBC NEWS (Aug. 9, 2021), https://www.nbcnews.com/tech/tech-news/twitters-racist-algorithm-also-ageist-ableist-islamaphobic-researchers-rcna1632.

[115] *See* SERVING COMMUNITIES OF COLOR, *supra* note 39, at 37; Catherine Zhu, *Dark Patterns—A New Frontier in Privacy Regulation*, REUTERS (July 29, 2021), https://www.reuters.com/legal/legalindustry/dark-patterns-new-frontier-privacy-regulation-2021-07-29/.

[116] *See* Olivia Solon, *Facebook Ignored Racial Bias Research, Employees Say*, NBC NEWS (July 23, 2020), https://www.nbcnews.com/tech/tech-news/facebook-management-ignored-internal-research-showing-racial-bias-current-former-n1234746.

[117] *See* Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[118] Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, HARV. BUS. REV. (Nov. 8, 2019), https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias).

These companies included retailers such as Walmart and Macy's, large data brokers like LiveRamp, and major credit reporting entities.[119] This data is often then used by such companies to target consumers for specific opportunities based on their unique characteristics, preferences, and behaviors.

- Amazon's same-day delivery service excluded predominantly Black ZIP codes in Atlanta, Boston, Chicago, Dallas, New York, and Washington. For example, in Boston, three ZIP codes in the primarily Black neighborhood of Roxbury were excluded from same-day service, but the neighborhoods surrounding Roxbury on all sides were eligible.[120]

- Leading automated speech recognition software from Amazon, Apple, Google, IBM, and Microsoft are all less accurate when processing the speech of Black Americans.[121]

- Black influencers drive popular trends on TikTok but do not equitably share in the profits created by their monetized content.[122]

- Weak app privacy can enable harmful third-party surveillance in public places. For example, a Catholic media outlet acquired a senior priest's cellphone data concerning his use of Grindr and tracking data regarding his visits to gay bars, causing him to resign.[123] Some of the individuals behind that incident were part of a larger effort by an organization that spent at least $4 million to collect and review data spanning several years from multiple dating apps in order to identify and expose gay priests.[124]

- Racially biased surveillance tools used in retail stores can lead to the discriminatory denial of service. For instance, the Federal Trade Commission

[119] Jon Keegan, *Each Facebook User is Monitored by Thousands of Companies*, THE MARKUP (Jan. 17, 2024), https://themarkup.org/privacy/2024/01/17/each-facebook-user-is-monitored-by-thousands-of-companies-study-indicates.
[120] David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERG (Apr. 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day/.
[121] Allison Koenecke et al., *Racial Disparities in Automated Speech Recognition*, 117 PNAS 7684 (2020), https://www.pnas.org/doi/10.1073/pnas.1915768117.
[122] Taylor Lorenz & Laura Zornosa, *Are Black Creators Really on 'Strike' From TikTok?*, N.Y. TIMES (Sept. 3, 2021), https://www.nytimes.com/2021/06/25/style/black-tiktok-strike.html.
[123] *See* Michelle Boorstein et al., *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), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.
[124] Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data that Tracked Gay Priests*, WASH. POST (Mar. 9, 2023), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/.

recently settled a case against the pharmacy chain Rite Aid for using facial recognition technology to erroneously identify women and people of color as potential shoplifters.[125] The inaccuracies in the tool used by Rite Aid led to significantly higher rates of false matches for Black, Latino, Asian, and women consumers, often leading employees to confront consumers and even refer individuals to law enforcement.[126]

H. Online hate, harassment, and threats

- 52% of U.S. adults reported personally experiencing online harassment, largely through social media.[127] Over half of people of color who experienced online harassment say they were targeted because of their race or ethnicity, compared to 18% of white targets.[128] 37% of all adults have experienced physical threats, sustained harassment, stalking, sexual harassment, doxing, or swatting, with 28% of lesbian, gay, or bisexual adults experiencing some form of severe harassment.[129] 58% of all teens have experience online harassment and 39% report experiences of severe harassment.[130] Hate, harassment, and discrimination inhibit the free speech and full participation of affected communities. Beyond direct exclusion, many will preemptively self-censor and withdraw for fear of being targeted. This in turn inhibits these communities' full and equal enjoyment of businesses supposedly open to the general public.[131]

- Online dating carries greater risks for people of color and LGBTQI+ users. "Black users were more likely than White users to be sent explicit images or messages, and lesbian, gay and bisexual daters experienced more harassment of all kinds

[125] Complaint for Permanent Injunction and Other Relief at 2, 23, *Fed. Trade Comm'n v. Rite Aid Corp.*, No. 23-cv-05023 (E.D. Pa. Dec. 19, 2023), ECF No. 1, https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf.

[126] *Id.* at 23–24.

[127] *See Online Hate and Harassment: The American Experience 2023*, ANTI-DEFAMATION LEAGUE CTR. FOR TECH. & SOC. 5 (June 2023), https://www.adl.org/sites/default/files/pdfs/2023-06/Online-Hate-and-Harassmen-2023_0.pdf.

[128] *Id.* at 32.

[129] *Id.* at 15, 35.

[130] *Id.* at 44.

[131] *See* Lindsay Mahowald, *LGBTQ People of Color Encounter Heightened Discrimination*, CTR. FOR AM. PROG. (Jun 24, 2021), https://www.americanprogress.org/article/lgbtq-people-color-encounter-heightened-discrimination/ (LGBTQ+ people of color report high rates of avoiding businesses so as not to experience discrimination.).

compared to straight daters. Overall, White users were more likely to say they felt safe dating online than Black, Hispanic and Asian adults."[132]

- In a global survey of women journalists, UNESCO and the International Center for Journalists found that 73% reported experiencing online violence, primarily on Facebook and Twitter, including threats of death, sexual violence, and violence against family members.[133] For 20%, online threats turned into offline attacks or abuse. Disinformation narratives fuel misogynistic attacks.[134] Black women journalists experience significantly disproportionate rates of online violence (81%) compared to white counterparts (64%), as do lesbian (88%) and bisexual (85%) women journalists compared to their straight counterparts (72%).[135] "Attacking women journalists is a fast, easy way to generate engagement on social media, experts say. Platforms reward outrage."[136] "Many who are targeted report on the internet itself and how it is being used to bolster extremists."[137]

- Platform algorithms help white supremacists connect with each other and systematically promote divisive material in the pursuit of maximizing user engagement.[138] An internal Facebook study noted that "64% of all extremist group joins are due to our recommendation tools . . . [o]ur recommendation systems grow the problem."[139] The study also concluded, "Our algorithms exploit the human brain's attraction to divisiveness" and will feed users "more and more divisive content in an effort to gain user attention [and] increase time on the platform."[140]

[132] Heather Kelly, *Finding Love, Sex and Harassment on Dating Apps*, WASH. POST (Feb. 6, 2023), https://www.washingtonpost.com/technology/2023/02/02/dating-apps-pew/.
[133] Julie Posetti et al., *The Chilling: A Global Study of Online Violence Against Women Journalists*, INT'L CTR. FOR JOURNALISTS 34 (Julie Posetti & Nabeelah Shabbir eds., Nov. 2, 2022), https://www.icfj.org/sites/default/files/2022-11/ICFJ_UNESCO_The%20Chilling_2022_1.pdf.
[134] *Id.* at 23, 32, 85.
[135] *Id.* at 47–48.
[136] Taylor Lorenz, *These Women Journalists Were Doing Their Jobs. That Made Them Targets*, WASH. POST (Feb. 14, 2023), https://www.washingtonpost.com/investigations/2023/02/14/women-journalists-global-violence/.
[137] *Id.*
[138] *See* Steve Rathje et al., *Out-group Animosity Drives Engagement on Social Media*, 118 PNAS (2021), https://www.pnas.org/doi/full/10.1073/pnas.2024292118; Keach Hagey & Jeff Horwitz, *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead.*, WALL ST. J. (Sept. 15, 2021), https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215 ("Internal memos show how a big 2018 change rewarded outrage and that CEO Mark Zuckerberg resisted proposed fixes.").
[139] Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*, WALL ST. J. (May 26, 2020), https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499?mod=hp_lead_pos5.
[140] *Id.*

When these issues were raised to Facebook executives, they declined to make changes.[141]

- YouTube video recommendations systematically recommend harmful and progressively more extreme content to viewers, creating pathways to white supremacy and hate group recruitment.[142]

- Following the murder of George Floyd by Minneapolis police, racist disinformation about his death surged on Facebook, YouTube, and Twitter.[143]

- Twitter saw an unprecedented rise in hate speech and disinformation following Elon Musk's takeover of Twitter, with the daily average number of slurs against Black Americans tripling on the platform.[144] Musk also restored hundreds of previously-banned extremist accounts, a move that may be due in part to ad revenues: one estimate said Twitter could make an estimated $19 million from just ten influential extremist accounts that were restored.[145]

[141] *See id.*

[142] *See* Rebecca Lewis, *Alternative Influence: Broadcasting the Reactionary Right on YouTube*, DATA & SOC'Y (Sept. 18, 2018), https://datasociety.net/library/alternative-influence/; Manoel Horta Ribeiro et al., *Auditing Radicalization Pathways on YouTube*, PROC. 2020 CONF. ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 131–41 (Jan. 2020), https://dl.acm.org/doi/abs/10.1145/3351095.3372879; MOZILLA FOUND., *YouTube Regrets: A Crowdsourced Investigation into YouTube's Recommendation Algorithm* (July 2021), https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf

[143] Davey Alba, *Misinformation About George Floyd Protests Surges on Social Media*, N.Y. TIMES (June 22, 2020), https://www.nytimes.com/2020/06/01/technology/george-floyd-misinformation-online.html.

[144] Drew Harwell, *Racist Tweets Quickly Surface After Musk Closes Twitter Deal*, WASH. POST (Oct. 28, 2022), https://www.washingtonpost.com/technology/2022/10/28/musk-twitter-racist-posts/; Sheera Frankel & Kate Conger, *Hate Speech's Rise on Twitter is Unprecedented, Researchers Find*, N.Y. TIMES (Dec. 2, 2022), https://www.nytimes.com/2022/12/02/technology/twitter-hate-speech.html; *see also, e.g.*, Carl Miller et al., *Antisemitism on Twitter Before and After Elon Musk's Acquisition*, INST. FOR STRATEGIC DIALOGUE & CASM TECH. (Mar. 20, 2023), https://www.isdglobal.org/wp-content/uploads/2023/03/Antisemitism-on-Twitter-Before-and-After-Elon-Musks-Acquisition.pdf ("English-language antisemitic Tweets more than doubled."); Katie Paul & Sheila Dang, *Exclusive: Twitter Leans on Automation to Moderate Content as Harmful Speech Surges*, REUTERS (Dec. 5, 2022), https://www.reuters.com/technology/twitter-exec-says-moving-fast-moderation-harmful-content-surges-2022-12-03/; Cat Zakrzewski et al., *Twitter Dissolves Trust and Safety Council*, WASH. POST (Dec. 12, 2022), https://www.washingtonpost.com/technology/2022/12/12/musk-twitter-harass-yoel-roth/.

[145] *See* Taylor Lorenz, *Extremist Influencers Are Generating Millions for Twitter, Report Says*, WASH. POST (Feb. 9, 2023), https://www.washingtonpost.com/technology/2023/02/09/twitter-ads-revenue-suspended-account/; *see also* CTR. FOR DIGIT. HATE, *Toxic Twitter: How Twitter Generates Millions in Ad Revenue by Bringing Back Banned Accounts*, (Feb. 9, 2023), https://counterhate.com/research/toxic-twitter/.

- Large language models and other AI trained on real-world data sets capture and reproduce racist stereotypes and biases.[146] Hateful autocomplete recommendations in Google Search are a highly visible manifestation of this problem.[147] As is Google's photo-categorization software labeling Black people as gorillas, which Google failed to fix for years.[148] Google's fix was to stop labelling gorillas altogether, rather than undertake a robust effort to diversify datasets and mitigate biases. Other companies took a similar approach to preempt public scrutiny, and eight years after the initial emergence of the problem with Google, neither Google nor Apple's photo-labelling software can identify gorillas.[149]

- An AI chatbot developed by Google produced racist responses that included impressions and stereotypes. The company did not adequately invest in diversity or AI ethics, according to a fired engineer.[150]

- Facebook profits from running ads on searches for hate group pages.[151] Google's ad network has been manipulated to help monetize websites that promote violence and misinformation.[152] Both have previously allowed ad targeting based on racism and hate speech.[153]

[146] *See* Moin Nadeem et al., *StereoSet: Measuring Stereotypical Bias in Pretrained Language Models*, In *Proc. 59th Ann. Meeting of the Ass'n for Computational Linguistics & 11th Int'l Joint Conf. on Nat. Language Processing*, ASS'N FOR COMPUTATIONAL LINGUISTICS 5356–71 (2021), https://arxiv.org/pdf/2004.09456.pdf.

[147] Issie Lapowsky, *Google Autocomplete Still Makes Vile Suggestions*, WIRED (Feb. 12, 2018), https://www.wired.com/story/google-autocomplete-vile-suggestions/.

[148] Tom Simonite, *When It Comes to Gorillas, Google Photos Remains Blind*, WIRED (Jan. 11, 2018), https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/.

[149] Nico Grant & Kashmir Hill, *Google's Photo App Still Can't Find Gorillas. And Neither Can Apple's*, N.Y. TIMES (May 22, 2023), https://www.nytimes.com/2023/05/22/technology/ai-photo-labels-google-apple.html.

[150] Urooba Jamal, *An Engineer Who Was Fired by Google Says Its AI Chatbot is 'Pretty Racist' and that AI Ethics at Google Are a 'Fig Leaf'*, BUS. INSIDER (July 31, 2022), https://www.businessinsider.com/google-engineer-blake-lemoine-ai-ethics-lamda-racist-2022-7.

[151] Naomi Nix, *Facebook Bans Hate Speech But Still Makes Money from White Supremacists*, WASH. POST (Aug. 10, 2022), https://www.washingtonpost.com/technology/2022/08/10/facebook-white-supremacy-ads/.

[152] *See* Craig Silverman & Isaac Arnsdorf, *How Steve Bannon Has Exploited Google Ads to Monetize Extremism*, PROPUBLICA (Nov. 29, 2021), https://www.propublica.org/article/how-steve-bannon-has-exploited-google-ads-to-monetize-extremism.

[153] *See* Sapna Maheshwari & Alexandra Stevenson, *Google and Facebook Face Criticism for Ads Targeting Racist Sentiments*, N.Y. TIMES (Sept. 15, 2017), https://www.nytimes.com/2017/09/15/business/facebook-advertising-anti-semitism.html.

- Commercial surveillance tools are used by domestic abusers and stalkers to track, threaten, and harm their targets.[154]

- Approximately 77% of American adults agree that misinformation increases hate crimes, including violence on the basis of race, gender, or religion; and 74% believe that misinformation in general is a major problem.[155]

- Facebook was instrumental in enabling the genocide of Rohingya Muslims in Myanmar.[156]

- Internal documents leaked from Facebook show that the platform was a central vehicle for promoting anti-Muslim hate and calls for violence that fueled deadly riots in India.[157]

- Facebook allowed ads to run in Kenya that promoted ethnic cleansing in the run-up to a national election.[158]

- Facebook was sued for $2 billion in a class-action alleging that Facebook played a role in the proliferation of violent political content on its platform in Ethiopia. The suit alleged that there is a disparity between content moderation resources that Facebook dedicates to African countries compared to the United States.[159]

[154] Sarah Jeong, *Surveillance Begins at Home*, FORBES: TECH (Oct. 28, 2014), https://www.forbes.com/sites/sarahjeong/2014/10/28/surveillance-begins-at-home/.

[155] David Klepper, *Poll: Most in US Say Misinformation Spurs Extremism, Hate*, ASSOCIATED PRESS (Oct. 13, 2022), https://apnews.com/article/religion-crime-social-media-race-and-ethnicity-05889f1f4076709c47fc9a18dbee818a.

[156] *See* Paul Mozur, *A Genocide Incited on Facebook, With Posts From Myanmar's Military*, N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html; Dan Milmo, *Rohingya Sue Facebook for £150bn Over Myanmar Genocide*, THE GUARDIAN (Dec. 6, 2021), https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence; Tom Miles, *U.N. Investigators Cite Facebook Role in Myanmar Crisis*, REUTERS (Mar. 12, 2018), https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN;

[157] *See* Newley Purnell & Jeff Horwitz, *Facebook Services Are Used to Spread Religious Hatred in India, Internal Documents Show*, WALL ST. J. (Oct. 23, 2021), https://www.wsj.com/articles/facebook-services-are-used-to-spread-religious-hatred-in-india-internal-documents-show-11635016354.

[158] Dell Cameron, *Facebook Approved Pro-Genocide Ads in Kenya After Claiming to Foster 'Safe and Secure' Elections*, GIZMODO (July 29, 2022), https://gizmodo.com/facebook-kenya-pro-genocide-ads-hate-speech-suspension-1849348778.

[159] Eli M. Rosenberg, *Facebook Hit with $2 Billion Lawsuit Connected to Political Violence in Africa*, NBC NEWS (Dec. 13, 2022), https://www.nbcnews.com/tech/misinformation/facebook-lawsuit-africa-content-moderation-violence-rcna61530.

- Extremism researchers have uncovered growing links between Russian disinformation and online extremism, finding that Russian disinformation feeds into narratives about white nationalism and is amplified by extremists across online networks. The number of links to Russian state-owned media domains on Gab and 4chan together are nearly level with those on VKontakte, Russia's leading social media platform.[160]

- Following the May 14, 2022, attack on the Black community in Buffalo that left ten Black people dead, the New York Attorney General published a report which found that online memes helped the shooter learn about the "great replacement" white supremacist conspiracy theory; online platforms were formative in his ideology of hate; and the shooter used online platforms to plan his attack, equip his arsenal, and livestream his violence.[161]

I. Voter intimidation and election disinformation

- Algorithmic tools are already being used to create and disseminate mis- and disinformation in the 2024 elections, often targeted at Black voters and other voters of color. During the New Hampshire primaries, bad actors used AI to create robocalls of President Biden to discourage voters from showing up at the polls.[162] In another example, several prominent social media accounts shared false AI-generated images of Black Trump supports to encourage Black voters to support the former President.[163]

- Leading AI chatbots frequently produce misleading, inaccurate, and harmful election information. For instance, when five of leading text AI models were tested with 26 common questions about the elections, researchers found that 51% of answers were inaccurate, such as telling users that California voters can vote by

[160] Rhys Leahy et al., *Connectivity Between Russian Information Sources and Extremist Communities Across Social Media Platforms*, 4 FRONTIERS POL. SCI., art. no. 885362 at 6 (June 22, 2022), https://www.frontiersin.org/articles/10.3389/fpos.2022.885362/full; Sara Fischer, *Russian Media Drives Online Hate*, AXIOS (June 7, 2022), https://www.axios.com/2022/06/07/russian-media-online-hate-extremists-racism.

[161] OFF. OF THE N.Y. STATE ATT'Y GEN. LETITIA JAMES, INVESTIGATIVE REPORT ON THE ROLE OF ONLINE PLATFORMS IN THE TRAGIC MASS SHOOTING IN BUFFALO ON MAY 14, 2022 (Oct. 18, 2022), https://ag.ny.gov/sites/default/files/buffaloshooting-onlineplatformsreport.pdf.

[162] Alex Seitz-Wald & Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Democrats Not to Vote Tuesday*, NBC NEWS (Jan. 22, 2024), https://www.nbcnews.com/politics/2024-election/fake-joe-biden-robocall-tells-new-hampshire-democrats-not-vote-tuesday-rcna134984.

[163] Marianna Spring, *Trump Supporters Target Black Voters with Faked AI Images*, BBC (Mar. 4, 2024), https://www.bbc.com/news/world-us-canada-68440150.amp.

text (they cannot), and that 40% of answers were harmful, including responses that discouraged users from voting.[164]

- Those seeking to engage in voter suppression can use datasets of personal information combined with robocalls, robotexts, and other mass communications tools to microtarget and spread voter intimidation at a scale and low cost previously unimagined. In one prominent example from the 2020 election, two men sent over 80,000 robocalls targeted to Black voters, seeking to deter them from voting by mail.[165] They spent only $1,000 on the robocalls.[166] The court ruled this conduct violated the Voting Rights Act and the Ku Klux Klan Act of 1871.[167] The court stated in that case:

> Today, almost 150 years later, the forces and conflicts that animated Congress's adoption of the Ku Klux Klan Act as well as subsequent voting rights legislation, are playing out again before this Court, though with a difference. In the current version of events, the means Defendants use to intimidate voters, though born of fear and similarly powered by hate, are not guns, torches, burning crosses, and other dire methods perpetrated under the cover of white hoods. Rather, Defendants carry out electoral terror using telephones, computers, and modern technology adapted to serve the same deleterious ends. Because of the vastly greater population they can reach instantly with false and dreadful information, contemporary means of voter intimidation may be more detrimental to free elections than the approaches taken for that purpose in past eras, and hence call for swift and effective judicial relief.[168]

[164] Julia Angwin et al., *Seeking Reliable Election Information? Don't Trust AI*, PROOF (Feb. 27, 2024), https://www.proofnews.org/seeking-election-information-dont-trust-ai/.

[165] *See Nat'l Coal. on Black Civic Participation v. Wohl*, 498 F. Supp. 3d 457 (S.D.N.Y. 2020).

[166] Memorandum of Law in Support of Plaintiffs' Joint Motion for Summary Judgment as to Liability on All Claims at 1, *Nat'l Coal. on Black Civic Participation v. Wohl*, Case No. 20-cv-8668 (July 29, 2022), ECF No. 213.

[167] *Nat'l Coal. on Black Civic Participation v. Wohl*, No. 20-cv-8668, __ F. Supp. 3d __, 2023 WL 2403012 (S.D.N.Y. Mar. 8, 2023) (granting affirmative summary judgment).

[168] *Nat'l Coal. on Black Civic Participation*, 498 F. Supp. 3d at 464.

The court also found the Defendants' message itself invoked the specter of surveillance to intimidate voters, noting that "[v]oter privacy is . . . vital to election integrity."[169]

- A right-wing social media influencer was convicted of conspiring with other Twitter users to spread deceptive images and tweets to supporters of Hillary Clinton during the 2016 election cycle. The images and tweets falsely suggested that voters could cast their votes via text message or social media. The convicted influencer, who was ranked as the 107th-most important influencer for the 2016 presidential election by MIT Media Lab, had specifically discussed the importance of limiting "black turnout" and targeting suppressive messaging towards "Black social spaces."[170] One of the images posted as part of the disinformation campaign was falsely framed as a Clinton campaign ad depicting a Black woman with an "African Americans for Hillary" sign and encouraging voters to "Avoid the Line" and "Vote from Home."[171]

- The Russian government used social media platforms to attempt to interfere in the 2016 U.S. election, including specifically targeting content to Black Americans intended to undermine confidence in the election and dissuade them from voting.[172] The campaign also used racially divisive issues in targeted ads.[173] Foreign adversaries used conventional advertising and targeting tools on social

[169] *Nat'l Coal. on Black Civic Participation*, 2023 WL 2403012, at *22.
[170] ASSOCIATED PRESS, *Far-right Influencer Convicted in Voter Suppression Scheme*, Politico (Mar. 31, 2023), https://www.politico.com/news/2023/03/31/far-right-influencer-convicted-in-voter-suppression-scheme-00090042; Colin Moynihan, *Trump Supporter Convicted in 2016 Scheme to Suppress Votes for Clinton*, N.Y. TIMES (Mar. 31, 2023), https://www.nytimes.com/2023/03/31/nyregion/douglass-mackey-trial-twitter-misinformation.html.
[171] Press Release, U.S. Att'y's Off. for the E. Dist. of N.Y., Social Media Influencer Douglass Mackey Convicted of Election Interference in 2016 Presidential Race (Mar. 31, 2023), https://www.justice.gov/usao-edny/pr/social-media-influencer-douglass-mackey-convicted-election-interference-2016.
[172] *See* S. Rep. No. 116-290 (2020), https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures; Scott Detrow, *What Did Cambridge Analytica Do During The 2016 Election?*, NPR (Mar. 20, 2018), https://www.npr.org/2018/03/20/595338116/what-did-cambridgeanalytica-do-during-the-2016-election; *see also* Gregory Eady et al., *Exposure to the Russian Internet Research Agency Foreign Influence Campaign on Twitter in the 2016 US Election and Its Relationship to Attitudes and Voting Behavior*, 14 NATURE COMMC'NS 1, 9 (Jan. 9, 2023), https://www.nature.com/articles/s41467-022-35576-9 ("In a word, Russia's foreign influence campaign on social media may have had its largest effects by convincing Americans that its campaign was successful.").
[173] *See* Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, NEW KNOWLEDGE & S. SELECT COMM. ON INTEL. (Oct. 2019), https://digitalcommons.unl.edu/senatedocs/2/.

media,[174] showing the dangerous ways in which off-the-shelf targeted advertising tools can be abused.[175] Researchers and reporters have documented Facebook groups selling accounts already approved to run political ads, allowing bad actors to circumvent Facebook's identity verification process.[176]

- Social media plays a key role in disinformation campaigns that spread conspiracy theories and seek to undermine election integrity.[177] The structure of the platforms, their profiling of users, and the use of recommendation engines to maximize user engagement at all costs can create a perfect storm for the spread of disinformation and disenfranchisement.[178] Misinformation is often more likely to be engaged with and shared than factual information, and platforms with greater pathways for virality are more likely to amplify misinformation.[179] "[T]o tackle thorny issues like misinformation, [Facebook employees] often had to demonstrate that their proposed solutions wouldn't anger powerful partisans or come at the expense of Facebook's growth."[180]

- YouTube was more likely to recommend videos involving election fraud conspiracy theories to users known to be skeptical about election validity, amplifying fringe disinformation.[181] Its AI content moderation system struggled with combatting

[174] *See* Press Release, FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

[175] *See* Craig Silverman, *Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months*, PROPUBLICA (July 1, 2022), https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine.

[176] *See* Sarah Emerson & Emily Baker-White, *Facebook Has a Thriving Black Market of Fraudulent Ad Accounts, Passports and Driver's Licenses*, FORBES (Nov. 14, 2022), https://www.forbes.com/sites/sarahemerson/2022/11/11/facebook-fraud-passports-political-ads/?sh=432e30d6927f.

[177] *See* ELECTION INTEGRITY P'SHIP, *The Long Fuse: Misinformation and the 2020 Election* (2021), https://www.eipartnership.net/report.

[178] *See* Karen Hao, *How Facebook Got Addicted to Spreading Misinformation*, MIT TECH. REV. (Mar. 11, 2021), https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/; Jeff Horwitz, *Facebook's Former Elections Boss Now Questions Social Media's Impact on Politics*, WALL ST. J. (Jan. 8, 2022), https://www.wsj.com/articles/facebooks-former-elections-boss-now-questions-social-medias-impact-on-politics-11641648561.

[179] Steven Lee Myers, *How Social Media Amplifies Misinformation More than Information*, N.Y. TIMES (Oct. 13, 2022), https://www.nytimes.com/2022/10/13/technology/misinformation-integrity-institute-report.html.

[180] Kevin Roose et al., *Facebook Struggles to Balance Civility and Growth*, N.Y. TIMES (Jan. 7, 2021), https://www.nytimes.com/2020/11/24/technology/facebook-election-misinformation.html.

[181] David Ingram, *YouTube Pushed Trump Supporters Toward Voter Fraud Videos, Study Finds*, NBC NEWS (Sept. 1, 2022), https://www.nbcnews.com/tech/misinformation/youtube-pushed-trump-supporters-voter-fraud-videos-study-finds-rcna45708.

disinformation in the short-form YouTube Shorts and in Spanish language videos.[182]

- The proliferation of disinformation on social media was a major contributor to false narratives and conspiracy theories attacking the outcome of the 2020 election,[183] culminating in the violent attack on the U.S. Capitol on January 6, 2021.[184] In a leaked draft report, the congressional January 6 Select Committee described how platforms ranging from Facebook, Twitter, and YouTube to Parler, Gab, and 4Chan, failed to stop disinformation, violent rhetoric, and tactical organization by users leading up to the insurrection.[185] Following the attack, the major platforms have lost interest in self-regulating to combat election disinformation on their services, even when their staff sound the alarm internally.[186]

- In the leadup to the 2022 midterm elections, Truth Social, founded by former President Donald Trump, became "a key organizing platform for election deniers," including one group that used the platform to promote "stakeouts" of ballot drop boxes.[187] The voter intimidation tactic was also discussed on Twitter, Telegram, Gab, and Craigslist.[188]

[182] *See* Nico Grant, *YouTube May Have Misinformation Blind Spots, Researchers Say*, N.Y. TIMES (Nov. 5, 2022), https://www.nytimes.com/2022/11/05/technology/youtube-misinformation.html.

[183] *See* Craig Silverman et al., *Facebook Groups Topped 10,000 Daily Attacks on Election Before Jan. 6, Analysis Shows*, WASH. POST (Jan. 4, 2022), https://www.washingtonpost.com/technology/2022/01/04/facebook-election-misinformation-capitol-riot/.

[184] *See generally* Ryan Goodman & Justin Hendrix, *January 6 Clearinghouse*, JUST SEC. (Dec. 1, 2023), https://www.justsecurity.org/77022/january-6-clearinghouse/.

[185] *See* Cat Zakrzewski et al., *What the Jan. 6 Probe Found Out About Social Media, But Didn't Report*, WASH. POST (Jan. 17, 2023), https://www.washingtonpost.com/technology/2023/01/17/jan6-committee-report-social-media/.

[186] *See* Steven Lee Myers & Nico Grant, *Combating Disinformation Wanes at Social Media Giants*, N.Y. TIMES (Feb. 14, 2023), https://www.nytimes.com/2023/02/14/technology/disinformation-moderation-social-media.html; Sheera Frankel & Cecilia Kang, *As Midterms Loom, Elections Are No Longer Top Priority for Meta C.E.O.*, N.Y. TIMES (June 23, 2022), https://www.nytimes.com/2022/06/23/technology/mark-zuckerberg-meta-midterm-elections.html; Ryan Mac & Sheera Frankel, *Internal Alarm, Public Shrugs: Facebook's Employees Dissect Its Election Role*, N.Y. TIMES (Oct. 22, 2021), https://www.nytimes.com/2021/10/22/technology/facebook-election-misinformation.html.

[187] Stuart A. Thompson & Matthew Goldstein, *Truth Social's Influence Grows Despite Its Business Problems*, N.Y. TIMES (Nov. 7, 2022), https://www.nytimes.com/2022/11/01/technology/truth-social-conservative-social-app.html.

[188] *See* Tiffany Hsu & Stuart A. Thompson, *Hunting for Voter Fraud, Conspiracy Theorists Organize 'Stakeouts'*, N.Y. TIMES (Aug. 10, 2022), https://www.nytimes.com/2022/08/10/technology/voter-drop-

(footnotes continue on next page)

- Targeted advertising plays a key role in election disinformation and voter suppression. The ability to microtarget ads allows political actors to send suppressive messages to specific niches of the electorate without detection or transparency. In 2022, researchers ran an experiment submitting ads with blatantly false information about voting to platforms, finding that TikTok approved 90% of the ads.[189] In 2016, the Trump campaign's data team put 3.5 million Black voters into a category for people they sought to deter from voting and used that categorization for Facebook ad targeting.[190] The number of Black voters in the "[d]eterrence" category was disproportionate to their share of the electorate in the swing states being targeted. The campaign targeted Black voters with negative ads designed to suppress turnout. The full extent of the campaign is unknown because there was no transparency as to what ads were sent to whom.[191] Recent research indicates that the sophistication and scope of political microtargeting will only accelerate as generative AI makes it easier and cheaper to create customizable targeting at scale.[192]

- Disinformation on social media in non-English languages, particularly Spanish, was rampant in the 2020 and 2022 election cycles and continues to be a major problem.[193] For example, Facebook ads targeting Hispanic populations

box-conspiracy-theory.html; *see also* Sheera Frankel, *On Social Media, Hunting for Voter Fraud Becomes a Game*, N.Y. TIMES (Nov. 4, 2022), https://www.nytimes.com/2022/11/04/technology/voter-fraud-social-media-games.html.

[189] Jennifer Korn, *Facebook and TikTok Are Approving Ads with 'Blatant' Misinformation About Voting in Midterms, Researchers Say*, CNN (Oct. 21, 2022), https://www.cnn.com/2022/10/21/tech/facebook-tiktok-misinfo-ads/index.html.

[190] Channel 4 News Investigations Team, *Revealed: Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016*, Channel 4 News (Sept. 28, 2020), https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016.

[191] *Id.*

[192] Tim Bernard, *Study Suggests We Should Worry About Political Microtargeting Powered by Generative AI*, TECH POL'Y PRESS (Feb. 7, 2024), https://www.techpolicy.press/study-suggests-we-should-worry-about-political-microtargeting-powered-by-generative-ai/.

[193] *See* Tiffany Hsu, *Misinformation Swirls in Non-English Languages Ahead of Midterms*, N.Y. TIMES (Oct. 12, 2022), https://www.nytimes.com/2022/10/12/business/media/midterms-foreign-language-misinformation.html; Kari Paul, *Facebook Must Tackle 'Spanish Language Disinformation Crisis', Lawmakers Say*, THE GUARDIAN (Mar. 16, 2021), https://www.theguardian.com/technology/2021/mar/16/facebook-spanish-language-disinformation-congress; CBS NEWS MIAMI, *Researchers Find WhatsApp Disinformation Campaigns Targeting Hispanic Voters in South Florida* (Nov. 1, 2020), https://www.cbsnews.com/miami/news/researchers-find-whatsapp-disinformation-campaigns-targeting-hispanic-voters/; Sabrina Rodriguez & Marc Caputo, *'This is F—ing Crazy': Florida Latinos Swamped by Wild Conspiracy Theories*, POLITICO (Sept. 14, 2020), https://www.politico.com/news/2020/09/14/florida-latinos-disinformation-413923.

inaccurately described prominent American politicians as "communist" and compared them to socialist presidents in South America.[194]

- Ahead of the 2022 midterm elections, disinformation about election fraud, anti-discrimination policies, and reproductive rights saturated WeChat, a social media platform used by an estimated 60% of the Chinese American community.[195]

- Users searching Google in 2020 for terms such as "register to vote," "vote by mail," and "where is my polling place" were met with voter registration ads that charged users to register to vote while mining their data.[196]

- A political action committee linked to a former member of Congress sent robotexts to Kansas voters to trick them into voting contrary to their preferences on a ballot initiative seeking to remove legal protections for abortion.[197]

- Meta developed an AI chatbot, and within a few days of studying online chatter, it began spreading election denialism and antisemitic conspiracy theories.[198]

J. Government benefits and services

- Automated decision-making systems have erroneously disqualified individuals from food assistance benefits using a vague "criminal justice disqualification" criterion.[199] An algorithmic tool used by the Michigan Unemployment Insurance Agency to identify fraud in applications for unemployment benefits similarly incorrectly disqualified applicants.[200] And, in 2023, a federal judge ruled against

[194] *See* Amanda Seitz & Will Weissert, *Inside the 'Big Wave' of Misinformation Targeted at Latinos*, ASSOCIATED PRESS (Dec. 1, 2021), https://apnews.com/article/latinos-misinformation-election-334d779a4ec41aa0eef9ea80636f9595.

[195] Kimmy Yam, *Right-Wing Disinformation Ramps Up on WeChat Ahead of Midterms, Report Finds*, NBC NEWS (Oct. 3, 2022), https://www.nbcnews.com/news/asian-america/right-wing-disinformation-ramps-wechat-ahead-midterms-report-finds-rcna50539.

[196] CBS NEWS BAY AREA, *Google Removes Misleading Ads Related to Voting, Elections* (June 30, 2020), https://www.cbsnews.com/sanfrancisco/news/google-removes-misleading-ads-voting-elections/.

[197] Isaac Stanley-Becker, *Misleading Kansas Abortion Texts Linked to Republican-aligned Firm*, WASH. POST (Aug. 2, 2022), https://www.washingtonpost.com/politics/2022/08/02/kansas-abortion-texts/.

[198] Christianna Silva*, It Took Just One Weekend for Meta's New AI Chatbot to Become Racist*, MASHABLE (Aug. 8, 2022), https://mashable.com/article/meta-facebook-ai-chatbot-racism-donald-trump.

[199] Rashida Richardson et al., *Litigating Algorithms 2019 Report: New Challenges to Government Use of Algorithmic Decision Systems*, AI NOW INST. 19–20 (Sept. 2019), https://ainowinstitute.org/publication/litigating-algorithms-2019-u-s-report-2.

[200] *Id.* at 20.

Idaho for denying Medicaid recipients access to information about the function of an algorithmic tool used to allocate benefits.[201]

- An algorithmic tool used by the child welfare agency in Allegheny County, Pennsylvania flagged Black children for "mandatory" neglect investigations at disproportionately higher rates when compared with white children.[202] Another study found that the New York City child welfare agency failed to perform bias testing and institute other safeguards when using predictive modeling in child welfare services despite claims by the agency to the contrary.[203]

- ID.me, a vendor of identity verification services used by federal and state agencies to verify eligibility for unemployment insurance and other benefits, has led to widespread incorrect denials of benefits, particularly in communities of color.[204] ID.me's fraud detection services frequently require the use of facial recognition technology that is less accurate for people of color, and the IRS shelved a plan to use it for online services.[205] A year later, however, the IRS still did not have an alternative available.[206]

- Top tax filing websites sent sensitive data of online tax filers, including income and filing status, to Facebook through its Meta Pixel code, which is used to collect data for ad targeting.[207] Many Americans rely on these websites in large part due

[201] Press Release, ACLU of Idaho, Federal Court Rules Against Idaho Medicaid Program (Sept. 7, 2023), https://www.acluidaho.org/en/press-releases/federal-court-rules-against-idaho-medicaid-program.

[202] Sally Ho & Garance Burke, *An Algorithm That Screens for Child Neglect Raises Concerns*, AP News (Apr. 29, 2022), https://apnews.com/article/child-welfare-algorithm-investigation-9497ee937e0053ad4144a86c68241ef1.

[203] Roshan Abraham, *AI Use by Cops, Child Services In NYC Is a Mess: Report*, VICE: Motherboard (Feb. 22, 2023), https://www.vice.com/en/article/3adxak/nypd-child-services-ai-facial-recognition.

[204] *See, e.g.*, Letter from Sens. Ron Wyden, Cory Booker, Edward Markey, and Alex Padilla to FTC Chair Lina Kahn (May 18, 2022), https://www.wyden.senate.gov/imo/media/doc/Letter%20to%20FTC%20on%20ID.me%20deceptive%20statements%20051822.pdf.

[205] Tonya Riley, *A Year After Outcry, IRS Still Doesn't Offer Taxpayers Alternative to ID.me*, CYBERSCOOP (Feb. 9, 2023), https://cyberscoop.com/irs-facial-recognition-identity-privacy/.

[206] *Id.*; *see also* Natalie Alms & Aaron Boyd, *IRS Plans to Approve Use of Login-dot-gov as Tax Day Nears*, NEXTGOV/FCW (Mar. 13, 2023), https://www.nextgov.com/modernization/2023/03/plans-approve-use-login-dot-gov-tax-day-nears/383932/; Natalie Alms, *Planned Login-dot-gov Deployment at IRS is Postponed*, NEXTGOV/FCW (Mar. 27, 2023), https://www.nextgov.com/digital-government/2023/03/planned-login-dot-gov-deployment-irs-postponed/384476/; Khari Johnson, *A US Agency Rejected Face Recognition—and Landed in Big Trouble*, WIRED (Mar. 22, 2023), https://www.wired.com/story/a-us-agency-rejected-face-recognition-and-landed-in-big-trouble/.

[207] Simon Fondrie-Teitler et al., *Tax Filing Websites Have Been Sending Users' Financial Information to Facebook*, THE MARKUP (Nov. 28, 2022), https://themarkup.org/pixel-hunt/2022/11/22/tax-filing-websites-have-been-sending-users-financial-information-to-facebook.

to tax filing companies' long-running campaigns to obstruct government efforts to make tax filing free and to instead steer taxpayers towards paid filing services—campaigns that have significantly employed dark patterns and deceptive online advertising.[208]

- A study by academic researchers and Treasury Department officials found significant racial disparities in IRS audit-selection algorithms. These data-driven algorithms led Black taxpayers to be audited at 2.9 to 4.7 times the rate of non-Black taxpayers, even though the IRS does not collect race data.[209] This racial disparity is largely attributable to disparities in audits of taxpayers claiming the Earned Income Tax Credit (EITC), "the largest cash-based safety net program in the United States," and could be the result of audit-selection algorithms designed to focus on predicting whether a taxpayer will underreport at all rather than the size of their underreporting.[210] Among subgroups of EITC claiming taxpayers, unmarried Black men face the greatest disparity compared to their respective non-Black counterparts, facing audits at more than twice the rate.[211]

K. Policing and law enforcement access to commercial surveillance

- Software developed and sold to law enforcement and courts for so-called "predictive policing," risk assessments, and criminal sentencing has been shown time and again to be racially biased against Black Americans.[212] For example, one tool disproportionately predicted crime in neighborhoods that had higher populations of Black, Latino, and low-income residents, often predicting little to

[208] *See* Justin Elliott & Paul Kiel, *Inside TurboTax's 20-Year Fight to Stop Americans from Filing Their Taxes for Free*, PROPUBLICA (Oct. 17, 2019), https://www.propublica.org/article/inside-turbotax-20-year-fight-to-stop-americans-from-filing-their-taxes-for-free; Will Young, *TurboTax is Still Tricking Customers with Tax Prep Ads that Misuse the Word "Free"*, PROPUBLICA (Feb. 18, 2020), https://www.propublica.org/article/turbotax-is-still-tricking-customers-with-tax-prep-ads-that-misuse-the-word-free ("Intuit places its ads strategically in searches for 'IRS' and 'free file,' among thousands of related search terms.").

[209] Hadi Elzayn et al., *Measuring and Mitigating Racial Disparities in Tax Audits* 3–4 (Stan. Inst. for Econ. Pol'y Rsch. Working Paper, Jan. 30, 2023), https://dho.stanford.edu/wp-content/uploads/IRS_Disparities.pdf.

[210] *See id.* at 4–5, 10.

[211] *Id.* at 28–29.

[212] *See* Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to be Dismantled.*, MIT TECH. REV. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

no crime in wealthier, whiter neighborhoods.[213] The software company claimed its tool was free of bias because it did not include demographic information in its predictions. However, predictions were based on data of previously reported crimes, reflecting racial disparities in crime reporting and statistics. Available data also indicated higher arrest and use-of-force rates in neighborhoods with higher prediction rates, suggesting that the software reinforces existing disparities.[214]

- Facial recognition is widely used by law enforcement agencies despite well-established racial biases in the technology. Almost all known cases of wrongful arrest due to facial recognition have been of Black people—including a Black woman in Detroit who was wrongfully arrested when she was eight months pregnant even though the suspect was not pregnant, and a Black man in Georgia who had never been to Louisiana arrested for a crime in Louisiana.[215]

- In addition to the racial biases inherent to the technology itself, facial recognition is often deployed in a racially discriminatory manner. For instance, a survey of more than 25,000 CCTV cameras in New York City found that neighborhoods with a higher proportion of residents of color had a higher concentration of facial recognition-compatible CCTV cameras.[216] Another report recently found that the New Orleans Police Department disproportionately used facial recognition to identify Black individuals, deploying the technology on Black people over 90 percent of the time.[217]
- Many jurisdictions use algorithms to predict recidivism risk when setting probation conditions, with little transparency as to the formulas and criteria

[213] Aaron Sankin et al., *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, THE MARKUP (Dec. 2, 2021), https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[214] *Id.*

[215] *See* Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. TIMES (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/technology/facial-recognition-false-arrest.html; John Simerman, *JPSO Used Facial Recognition Technology to Arrest a Man. The Tech Was Wrong.*, NOLA.COM (Jan. 2, 2023), https://www.nola.com/news/crime_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article_0818361a-8886-11ed-8119-93b98ecccc8d.html; Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, WIRED (Feb. 28, 2023), https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/.

[216] AMNESTY INT'L, *USA: Facial Recognition Technology Reinforcing Racist Stop-and-Frisk Policing in New York–New Research* (Feb. 15, 2022), https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/.

[217] *See* Alfred Ng, *'Wholly Ineffective and Pretty Obviously Racist': Inside New Orleans' Struggle with Facial-Recognition Policing*, POLITICO (Oct. 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427.

considered.[218] The American Bar Association passed a resolution urging that pretrial risk assessment tools should not be used unless they can be proven to be unbiased.[219]

- Reliance on arrest records to train algorithms reproduces discrimination. An investigation of a predictive policing tool deployed in Oakland, California found that the tool produced racially biased estimates of illicit drug use because it relied on arrest records rather than on a "non-criminal justice, population-based data source" such as the National Survey on Drug Use and Health.[220]

- ShotSpotter, an audio gunshot detection technology, uses algorithms that are trained on data inputted by police officers.[221] ShotSpotter devices are overwhelmingly located in majority- or plurality-Black and Brown neighborhoods,[222] but there are significant doubts about their accuracy,[223] and the company has resisted transparency around its algorithms and systems.[224] ShotSpotter raises safety concerns about falsely triggering armed responses by

[218] *See* Cade Metz & Adam Satariano, *An Algorithm That Grants Freedom, or Takes It Away*, N.Y. TIMES (Feb. 6, 2020), https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html.

[219] Lyle Moran, *Pretrial Risk-assessment Tools Should Only Be Used if They're Transparent and Unbiased, Warns ABA House*, ABA J. (Feb. 14, 2022), https://www.abajournal.com/news/article/resolution-700.

[220] Kristian Lum & William Isaac, *To Predict and Serve?*, 13 SIGNIFICANCE 14, 15–16 (2016), https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2016.00960.x (discussing racial bias in predictive policing systems trained on arrest records).

[221] Garance Burke et al., *How AI-Powered Tech Landed Man in Jail with Scant Evidence*, ASSOCIATED PRESS (Mar. 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220; Fola Akinnibi & Sarah Holder, *In New York Neighborhood, Police and Tech Company Flout Privacy Policy, Advocates Say*, BLOOMBERG (Dec. 15, 2022), https://www.bloomberg.com/news/articles/2022-12-15/nyc-police-and-tech-company-flout-privacy-policy-advocates-say; *see also* Garance Burke & Michael Tarm, *Confidential Document Reveals Key Human Role in Gunshot Tech*, ASSOCIATED PRESS (Jan. 20, 2023), https://apnews.com/article/shotspotter-artificial-intelligence-investigation-9cb47bbfb565dc3ef110f92ac7f83862

[222] Todd Feathers, *Gunshot-Detecting Tech is Summoning Armed Police to Black Neighborhoods*, VICE: MOTHERBOARD (July 19, 2021), https://www.vice.com/en/article/88nd3z/gunshot-detecting-tech-is-summoning-armed-police-to-black-neighborhoods; Thomas McBrien et al., *Screened & Scored in the District of Columbia*, ELEC. PRIV. INFO. CTR. 21 (Nov. 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf.

[223] *See* Burke et al., *supra* note 221; OFF. OF INSPECTOR GEN., CITY OF CHICAGO, THE CHICAGO POLICE DEPARTMENT'S USE OF SHOTSPOTTER TECHNOLOGY 3 (Aug. 24, 2021), https://igchicago.org/wp-content/uploads/2021/08/Chicago-Police-Departments-Use-of-ShotSpotter-Technology.pdf (evidence of gun-related offense found in only 9.1% of ShotSpotter alerts that Chicago police responded to).

[224] *See* Jay Stanley, *Four Problems with the ShotSpotter Gunshot Detection System*, ACLU (Aug. 24, 2021), https://www.aclu.org/news/privacy-technology/four-problems-with-the-shotspotter-gunshot-detection-system.

anxious officers into predominantly Black neighborhoods and due process concerns about unreliable data being used as a basis for stops or arrests.[225]

- Ring, operated by Amazon, routinely and voluntarily provides police access to video recordings from its cameras.[226] The company has partnered with police departments and cities, providing them with free cameras and access to Ring's Neighbors app, a neighborhood watch-esque social media network, where officers can request users to voluntarily share footage from their cameras to assist investigations.[227] In exchange, departments agreed to promote Ring's products.[228] Several cities maintain subsidy programs, encouraging residents to install Ring cameras at little or no cost.[229]

- In Washington, D.C., the district's Department of Transportation uses automated traffic cameras for traffic enforcement, which are disproportionately placed in predominantly Black neighborhoods. This has led to significantly higher rates of moving violations levied against drivers in these neighborhoods.[230]

- Data brokers like LexisNexis and Thomson Reuters collect and sell personal data to law enforcement agencies, who use this information to locate, track, and arrest

[225] McBrien et al., *supra* note 222, at 21; *see generally* Harvey Gee, *"Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach*, 55 UNIV. MICH. J. L. REFORM 767 (2022), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2561&context=mjlr.

[226] *See, e.g.*, Letter from U.S. Sen. Ed Markey to Andrew Jassy, Chief Exec. Officer, Amazon.com, Inc. (June 14, 2022), https://www.markey.senate.gov/imo/media/doc/senator_markey_letter_to_amazon_on_ring_audio_and_law_enforcement.pdf; David Priest, *Ring's Police Problem Never Went Away. Here's What You Still Need to Know*, CNET (Sept. 27, 2021), https://www.cnet.com/home/security/rings-police-problem-didnt-go-away-it-just-got-more-transparent/; David Schwarz & Simon McCormack, *The NYPD Is Teaming Up With Amazon Ring. New Yorker's Should Be Worried*, NYCLU (Jan. 11, 2023), https://www.nyclu.org/en/news/nypd-teaming-amazon-ring-new-yorkers-should-be-worried.

[227] Alfred Ng, *The Privacy Loophole in Your Doorbell*, POLITICO (Mar. 07, 2023), https://www.politico.com/news/2023/03/07/privacy-loophole-ring-doorbell-00084979; *see also* Barry Friedman et al., *Ring Neighbors & Neighbors Public Safety Service: A Civil Rights & Civil Liberties Audit*, N.Y.U. POLICING PROJECT 17–21 (2021), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/61baab9fcc4c282092bbf7c3/1639623584675/Policing+Project+Ring+Civil+Rights+Audit+%28Full%29.pdf (explaining features of police access to Neighbors app).

[228] Matthew Guariglia & Karen Gullo, *Emails from 2016 Show Amazon Ring's Hold on the LAPD Through Camera Giveaways*, ELEC. FRONTIER FOUND. (June 17, 2021), https://www.eff.org/deeplinks/2021/06/emails-show-amazon-rings-hold-lapd-through-camera-giveaways; Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, VICE: MOTHERBOARD (July 25, 2019), https://www.vice.com/en/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement.

[229] Louise Matsakis, *Cops Are Offering Ring Doorbell Cameras in Exchange for Info*, WIRED (Aug. 2, 2019), https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/.

[230] McBrien et al., *supra* note 222, at 19.

individuals.[231] Both companies have provided Immigration and Customs Enforcement (ICE) with access to sensitive personal information, including financial information, marriage records, and addresses.[232] In a seven-month period, ICE ran over one million searches on their LexisNexis platforms.[233]

- The data broker Venntel has sold location data to the FBI, CBP, ICE, other components of DHS, and the IRS. This data has been used for everything from tax enforcement to the surveillance and tracking of migrants.[234]

- During the 2020 Black Lives Matter protests, a data broker, claiming access to data from over 1 billion devices, analyzed the location data of nearly 17,000 devices to infer protesters' race, gender, age, and hometowns.[235] The same broker

[231] *See* Joseph Cox, *LexisNexis 'Virtual Crime Center' Makes Millions Selling to the Government*, VICE: MOTHERBOARD (Feb. 2, 2023), https://www.vice.com/en/article/y3p8j5/lexisnexis-selling-data-government; Drew Harwell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, WASH. POST (Feb. 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/.

[232] *See* Cox, *supra* note 231; Nina Wang et al., *American Dragnet: Data-Driven Deportation in the 21st Century*, GEO. L. CTR. ON PRIV. & TECH. 16, 45–46 (2022), https://www.americandragnet.org/sites/default/files/American_Dragnet_report_English_final.pdf; *see also* Sam Biddle, *ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months*, THE INTERCEPT (June 9, 2022), https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/; Press Release, Ill. Coal. for Immigrant & Refugee Rts. et al., Activists Sue LexisNexis for Mass Collection and Sale of Personal Data of Millions (Aug. 16, 2022), https://www.icirr.org/News/activists-sue-lexisnexis-for-mass-collection-and-sale-of-personal-data-of-millions.

[233] Biddle, *supra* note 232.

[234] *See* Lee Fang, *FBI Expands Ability to Collect Cellphone Data, Monitor Social Media, Recent Contracts Show*, THE INTERCEPT (June 24, 2020), https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL ST. J. (June 19, 2020), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815; *see also* Joseph Cox, *CBP Refuses to Tell Congress How it is Tracking Americans Without a Warrant*, VICE (Oct. 23, 2020), https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant; *See* Byron Tau, *Treasury Watchdog Warns of Government Use of Cellphone Data Without Warrants*, WALL ST. J. (Feb. 22, 2021), https://www.wsj.com/articles/treasury-watchdog-warns-of-governments-use-of-cellphone-data-without-warrants-11614003868.

[235] Caroline Haskins, *Almost 17,000 Protesters Had No Idea a Tech Company Was Tracing Their Location*, BUZZFEED NEWS (June 25, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying.

has told Congress that data it is has sold to other brokers has subsequently been sold to law enforcement and the military.[236]

- Following the *Dobbs* decision overturning *Roe v. Wade*, data brokers refused to stop collecting information on pregnant people, which could be used to prosecute people seeking abortions.[237] Location data, search history, credit card transaction history, and other information about everyday activities can be used to identify someone who has sought out reproductive or LGBTQ+ healthcare.[238]

- Dataminr is a service built to scan through Twitter and other social media to surface real-time intelligence for law enforcement, investment firms, media outlets, and other organizations. Company insiders say it overamplified supposed criminal threats in a manner that amounted to racial profiling and stereotyping.[239]

- Amazon's social media crime-reporting app, Neighbors, routinely facilitates racial profiling, with people of color being reported as "suspicious." It also has forums rife with racism.[240]

- Facebook, Twitter, and Instagram provided user data to Geofeedia, a social media monitoring product that was marketed to law enforcement agencies to surveil civil rights activists.[241]

- Absent any specific restrictions, many companies can sell or share data with law enforcement, ranging from motels sharing guest data with ICE for immigration

[236] *See* Byron Tau, *How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies*, WALL ST. J. (Nov. 18, 2021), https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202.

[237] Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info on Pregnant People*, POLITICO (Aug. 1, 2022), https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988.

[238] *See, e.g.*, Adrian Astorgano, *From 'Heavy Purchasers' of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, THE MARKUP (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

[239] *See* Sam Biddle, *Twitter Surveillance Startup Targets Communities of Color for Police*, THE INTERCEPT (Oct. 21, 2020), https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling/.

[240] Caroline Haskins, *Amazon's Home Security Company Is Turning Everyone Into Cops*, VICE: MOTHERBOARD (Feb. 7, 2019), https://www.vice.com/en/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops.

[241] *See* Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU NORCAL (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

enforcement[242] to genealogy and DNA companies sharing genetic data with the FBI,[243] to federal agencies simply buying cell phone location data in bulk.[244]

- Geofence warrants[245] are increasingly being employed to exploit the large collections of users' location data amassed by tech companies like Google.[246] By its own numbers, Google received upwards of 10,000 geofence warrants in 2020, a more than 10 times increase since 2018.[247] Publicly reported cases suggest that police are using the warrants to make sweeping searches instead of taking less invasive steps to develop more particularized probable cause.[248]

- In recent years, law enforcement has increasingly served so-called keyword search warrants on search engine providers, broadly demanding data on anyone who

[242] Eli Rosenberg, *Motel 6 Will Pay $12 Million to Guests Whose Personal Data Was Shared with ICE*, WASH. POST (Apr. 6, 2019), https://www.washingtonpost.com/nation/2019/04/06/motel-leaked-personal-data-guests-ice-officials-say-now-it-owes-them-million/.

[243] Kristen V. Brown, *Major DNA Testing Company Sharing Genetic Data with the FBI*, BLOOMBERG: TECH.: PROGNOSIS (Feb. 1, 2019), https://www.bloomberg.com/news/articles/2019-02-01/major-dna-testing-company-is-sharing-genetic-data-with-the-fbi.

[244] *See* Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data*, ELEC. FRONTIER FOUND. (June 13, 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data; Joseph Cox, *Secret Service Bought Phone Location Data from Apps, Contract Confirms*, VICE: MOTHERBOARD (Aug. 17, 2020), https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street.

[245] *See generally* FOURTH AMEND. CTR., NAT'L ASS'N OF CRIM. DEF. LAWS., *Geofence Warrant Primer* (2022), https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf.

[246] *See, e.g.*, Cullen Seltzer, *Google Knows Where You've Been. Should It Tell the Police?*, SLATE (May 16, 2022), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html; *see also* Corin Faife, *FBI Used Geofence Warrant in Seattle After BLM Protest Attack, New Documents Show*, THE VERGE (Feb. 5, 2022), https://www.theverge.com/2022/2/5/22918487/fbi-geofence-seattle-blm-protest-police-guild-attack; Thomas Brewster, *Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson*, FORBES (Aug. 31, 2021), https://www.forbes.com/sites/thomasbrewster/2021/08/31/google-dragnets-on-phone-data-across-13-kenosha-protest-arsons/; Matthew Guariglia et al., *Geofence Warrants Threaten Civil Liberties and Free Speech Rights in Kenosha and Nationwide*, ELEC. FRONTIER FOUND. (Sept. 10, 2021), https://www.eff.org/deeplinks/2021/09/geofence-warrants-threaten-civil-liberties-and-free-speech-rights-kenosha-and. Apple, Snapchat, Uber, and Lyft have all reportedly received geofence requests as well. *See* Justin Jouvenal & Rachel Weiner, *Cellphone Dragnets Can Help Catch Criminals. Judges Say They Can Also Violate Constitutional Rights*, WASH. POST (Mar. 21, 2022), https://www.washingtonpost.com/dc-md-va/2022/03/21/geofence-search-warrant-judge-virginia/; Albert Fox Cahn, *This Unsettling Practice Turns Your Phone into a Tracking Device for the Government*, FAST CO. (Jan. 17, 2020), https://www.fastcompany.com/90452990/this-unsettling-practice-turns-your-phone-into-a-tracking-device-for-the-government.

[247] GOOGLE, *Supplemental Information on Geofence Warrants in the United States* (2021), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (see also the .csv data linked on page 2).

[248] *See* Sidney Fussell, *An Explosion in Geofence Warrants Threatens Privacy Across the US*, WIRED (Aug. 27, 2021), https://www.wired.com/story/geofence-warrants-google/.

searched for a particular set of terms.[249] In addition to raising Fourth and First Amendment concerns,[250] dragnet warrants may also expose those seeking reproductive healthcare information to prosecution.[251]

- ICE uses administrative subpoenas to obtain private records from tech and telecom companies.[252] About 86,000 subpoenas were sent to AT&T, T-Mobile, and Comcast; and about 15,000 were sent to tech companies, including Google, Meta, and Microsoft; a single ICE field office issued more than 1,000 subpoenas in a single day.[253] ICE has a notable history of dragnet surveillance,[254] and its efforts threaten to sweep more people into an immigration enforcement system that is inextricably tied to racism and racial disparities.[255]

- Even if an individual consents to share their data in a manner that could expose it to law enforcement, they cannot consent for others. Yet many forms of data made available—including contacts, addresses, genetic information, and associations—necessarily impinge the privacy of others as well, without their knowledge or consent.

[249] *See* Thomas Brewster, *Exclusive: Government Secretly Orders Google To Identify Anyone Who Searched A Sexual Assault Victim's Name, Address Or Telephone Number*, FORBES (Oct. 4, 2021), https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=443722997c97.

[250] *See id.*

[251] *See* Albert Fox Cahn & Julian Melendi, *The New Way Police Could Use Your Google Searches Against You*, SLATE (Aug. 1, 2022), https://slate.com/technology/2022/08/keyword-search-warrants-colorado-roe.html; *see also* Brief of Amicus Curiae Electronic Privacy Information Center in Support of Petitioner Gavin Seymour and Reversal at 5–9, *People v. Seymour*, 536 P.3d 1260 (Colo. 2023) (No. 2023SA12), https://epic.org/wp-content/uploads/2023/01/Seymour-v.-Colorado-CO-Supreme-Court.pdf.

[252] Dhruv Mehrotra, *ICE Is Grabbing Data From Schools and Abortion Clinics*, WIRED (Apr. 3, 2023), https://www.wired.com/story/ice-1509-custom-summons/.

[253] *Id.*

[254] *See generally* Wang et al., *supra* note 232.

[255] *See* Charles Kamasaki, *U.S. Immigration Policy: A Classic Unappreciated Example of Structural Racism*, BROOKINGS (Mar. 26, 2021), https://www.brookings.edu/blog/how-we-rise/2021/03/26/us-immigration-policy-a-classic-unappreciated-example-of-structural-racism/ (structural racism in immigration policy and law); Alison Leal Parker, *US Immigration Enforcement and US Obligations Under the International Convention on the Elimination of Racial Discrimination (ICERD): Written Testimony Submitted to the US State Department and other Federal Agencies*, HUM. RTS. WATCH (Apr. 28, 2022), https://www.hrw.org/news/2022/04/28/us-immigration-enforcement-and-us-obligations-under-international-convention (racial disparities in immigration enforcement).