



**LAWYERS' COMMITTEE FOR  
CIVIL RIGHTS  
U N D E R L A W**

**STATEMENT OF DAMON T. HEWITT  
PRESIDENT AND EXECUTIVE DIRECTOR  
LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW**

**U.S. SENATE COMMITTEE ON THE JUDICIARY  
SUBCOMMITTEE ON  
COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS**

**HEARING ON  
"THE NEW INVISIBLE HAND? THE IMPACT OF ALGORITHMS ON  
COMPETITION AND CONSUMER RIGHTS"**

**DECEMBER 13, 2023**

## I. Introduction

Chair Klobuchar, Ranking Member Lee, and Members of the Subcommittee, thank you for the opportunity to testify today about the impact of algorithms on consumer and civil rights. My name is Damon T. Hewitt, and I am the President and Executive Director of the Lawyers' Committee for Civil Rights Under Law ("Lawyers' Committee").

The Lawyers' Committee is a nonpartisan, nonprofit organization, formed in 1963 at the request of President John F. Kennedy to mobilize the nation's leading lawyers as agents for change in the Civil Rights Movement. Today, we use 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, privacy, and technology to address predatory data practices, discriminatory algorithms, and other online harms that disproportionately affect people of color.

Equal opportunity and civil rights are intertwined with technological advancement. In the consumer context, algorithms are used 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, digital redlining, and pervasive surveillance.

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 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.

Algorithmic collusion and discrimination present a stark market barrier between the promise of what is, and what could be. The harms of algorithmic discrimination are already denying millions of Americans equal opportunity in our economy. Instead of aiding consumers, AI tools too often create distortions in the marketplace, reflecting exclusion rather than fairness for consumers and creating closed doors in the virtual world that have discriminatory effects in real life. Left unchecked, these harmful impacts will continue to grow as AI becomes engrained in every aspect of our lives.

Just as the struggles of the civil rights movement culminated in milestone civil rights laws, so too does this struggle need to culminate in new protections. The time has come for Congress to enact legislation ensuring the algorithmic systems are safe, effective, and fair. Legislation needs to center civil rights, establish baseline protections for consumers and their privacy, and empower effective oversight.

*First*, AI regulation should protect Americans' civil rights. Legislation should establish anti-discrimination protections to close gaps in existing law created by novel online and algorithmic contexts. It should also require pre- and post-deployment testing requirements to evaluate algorithmic systems for discrimination and bias. All too often, consumers—especially Black and Brown consumers—end up as unwilling test subjects for unsafe algorithms and consumer technologies. Algorithmic harm needs to be identified, prevented, and mitigated as a fundamental part of the development process.

*Second*, AI legislation should establish baseline consumer protections. These should include a duty of care to require that products are safe and effective, data privacy to protect consumers' personal information, and transparency and explainability requirements so that consumers know when, how, and why, AI is being used. Consumers should be empowered to make fully informed decisions about how they interact with algorithmic systems and companies should take adequate steps to make sure that their products work as intended.

*Third*, AI regulation should establish robust oversight and enforcement. Congress should empower a federal regulator with adequate authority and resources and provide a private right of action to remedy algorithmic harms. Black people and other people of color historically have not been able to rely upon the government to protect their interests, so individuals need to be able to vindicate their own rights.

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, alongside other legislation to address discrimination in employment, housing, and other critical aspects of Americans' lived experiences in the marketplace. Today, the mass generation and collection of personal data through the internet and the use of algorithmic technologies to determine

economic opportunities create new challenges to the prevention and elimination of discrimination. It is time to build upon our civil rights infrastructure to ensure that everyone has equal opportunity in the new digital marketplace and fair access to the information, goods, and services it enables.

## II. Segregation and Redlining Produced Inequities that Persist Today and Affect the Data Flowing In and Out of Algorithmic Systems

It should be no surprise that when you draw data from a society with a bedrock history of systemic inequity, the data will be steered by that history. Generations of institutionalized oppression of Black Americans—through slavery, segregation, redlining, and disenfranchisement—is an inescapable part of American history whose present-day effects are embedded in the foundation of our society.

Contemporary commercial surveillance practices that undergird modern algorithmic tools originated in this separate-but-equal segregation, which denied equal opportunity to millions of Black people. The analog version of a discriminatory algorithm was redlining, which deprived Black people of intergenerational wealth and health. This one historic algorithmic system—using racial geography as part of a formula for determining government subsidies for homeownership, built on top of segregated housing—has caused a *century* of devastating downstream effects with no end in sight.

The consequences of residential and educational segregation are still with us.<sup>1</sup> Disparities in employment and credit opportunities, and resulting disparities in intergenerational wealth generation, are still endemic.<sup>2</sup> Access to healthcare and clean environments is unequal.<sup>3</sup> The ongoing consequences of segregation are legion:

---

<sup>1</sup> See, e.g., Patrick Sharkey, *Stuck in Place: Urban Neighborhoods and the End of Progress Toward Racial Equality* 9–10, 91–116 (Univ. of Chicago Press 2013); Roslyn Arlin Mickelson, *Exploring the School-Housing Nexus: A Synthesis of Social Science Evidence*, in *Finding Common Ground: Coordinating Housing and Education Policy to Promote Integration* 5 & n.1 (Philip Tegeler ed., Poverty & Race Rsch. Action Council & Nat'l Coal. on Sch. Diversity 2011), <http://www.prrac.org/pdf/HousingEducationReport-October2011.pdf>.

<sup>2</sup> See, e.g., Michael A. Stoll, *Job Sprawl and the Spatial Mismatch between Blacks and Jobs*, Brookings Inst. Metro. Pol'y Program 7 (Feb. 2005), <https://www.brookings.edu/research/job-sprawl-and-the-spatial-mismatch-between-blacks-and-jobs/>; Rashawn Ray et al, *Homeownership, Racial Segregation, and Policy Solutions to Racial Wealth Equity*, Brookings (Sept. 1, 2021), <https://www.brookings.edu/articles/homeownership-racial-segregation-and-policies-for-racial-wealth-equity/>.

<sup>3</sup> See, e.g., Sherman A. James, *John Henryism and the Health of African-Americans*, 18 *Culture, Med., & Psych.* 163–82 (1994), <https://doi.org/10.1007/BF01379448>; Ctr. for Fam. Rsch., *Skin-deep Resilience Research Digest*, Univ. of Ga., <https://cfr.uga.edu/for-researchers/research-digests/skin-deep-resilience/>; Helen H. Kang, *Pursuing Environmental Justice: Obstacles and Opportunities – Lessons from the Field*, 31 *Wash. U. J. L. & Pol'y* 121, 126–67 (2009); U.S. ENV'T. PROT. AGENCY, *Environmental Equity: Reducing Risk for All Communities* 15 (1992), [https://www.epa.gov/sites/default/files/2015-02/documents/reducing\\_risk\\_com\\_vol1.pdf](https://www.epa.gov/sites/default/files/2015-02/documents/reducing_risk_com_vol1.pdf).

“investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates; and the list goes on.”<sup>4</sup>

The effects of discrimination are literally shortening the lives and health-spans of Black Americans, manifesting as disproportionate incidences of inflammatory diseases.<sup>5</sup> As the Supreme Court has held, destroying the badges and incidents of slavery “at the very least” necessitates “the freedom to buy whatever a white man can buy, the right to live wherever a white man can live.”<sup>6</sup>

These effects now manifest in data about Black communities and other communities of color—data that will be 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.

### **III. Inheriting the Mistakes of the Past: How Algorithmic Systems Disproportionately Harm and Discriminate Against Black Communities and Other Communities of Color**

In a society scaffolded on top of the consequences of institutionalized oppression, algorithmic systems often reproduce discrimination. At the root of algorithmic bias is the reckless, if not knowing or intentional, application of machine learning techniques to massive troves of data drawn from a society blighted by systemic inequity—and the lazy presumption that what came before is what will be. The through-lines for the data are often race, gender, and other immutable traits. When an algorithm executes its mission of creating efficiency by finding hidden correlations, it will often mistake the long-term consequences of discrimination and inequality for an individual’s preferences and traits.<sup>7</sup> These mistaken shortcuts fail to account for the fact that while a person may be in part a product of their

---

<sup>4</sup> *Leaders of a Beautiful Struggle v. Baltimore Police Dep’t*, 2 F.4th 330, 349 (4th Cir. 2021) (en banc) (Gregory, C.J., concurring).

<sup>5</sup> See, e.g., Sherman A. James, *John Henryism and the Health of African-Americans*, 18 *Culture, Med., & Psych.* 163–82 (1994), <https://doi.org/10.1007/BF01379448>; CTR. FOR FAM. RSCH., *Skin-deep Resilience Research Digest*, Univ. of Ga., <https://cfr.uga.edu/for-researchers/research-digests/skin-deep-resilience/>.

<sup>6</sup> *Jones v. Alfred H. Mayer Co.*, 392 U.S. 409, 443 (1968) (cleaned up).

<sup>7</sup> 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 and Demos (2021), [https://www.demos.org/sites/default/files/2021-05/Demos\\_%20D4BL\\_Data\\_Capitalism\\_Algorithmic\\_Racism.pdf](https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf).

circumstances, that does not mean they necessarily *are* or *should be* limited by those circumstances. Expediency is no excuse for segregation.

The bottom line is that if existing civil rights laws and agency resources were sufficient to address algorithmic discrimination, then the problem would not be pervasive in the first place. As a result of gaps in federal law, individuals currently have limited recourse against discriminatory algorithms and AI models used in commercial settings that reinforce the structural racism and systemic bias that pervade our society. Technology companies can misuse personal data, intentionally or unintentionally, to harm marginalized communities through deception, discrimination, exploitation, and perpetuation of redlining. Absent updated and robust anti-discrimination protections, online businesses may be able to deny service on the basis of race or ethnicity, provide subpar products based on gender or sexual orientation, charge higher rates based on religion, or ignore the accessibility needs of persons with disabilities.

“Just as neighborhoods can serve as a proxy for racial and ethnic identity, there are new worries that big data technologies could be used to ‘digitally redline’ unwanted groups, either as customers, employees, tenants, or recipients of credit.”<sup>8</sup> 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. Not surprisingly, extensive documentation demonstrates that consumers of color continue to receive worse treatment and experience unequal access to goods and services due to discriminatory algorithms and exploitative data practices. These harms are widespread across sectors, including housing, employment, credit, insurance, healthcare, education, retail, and public accommodations (see Appendix I).

In advertising, for example, Facebook (now known as Meta) allowed discrimination in the targeting and delivery of advertising for housing, credit services, and job openings based on race, sex, and age. The company was eventually forced to change its advertising targeting system as part of a legal settlement,<sup>9</sup> but was still charged with engaging in race discrimination by the Department of Housing and Urban Development.<sup>10</sup> In fact, Meta *literally* engaged in redlining—it allowed

---

<sup>8</sup> EXEC. OFF. OF THE PRESIDENT, *Big Data: Seizing Opportunities, Preserving Values* 53 (2014), [https://obamawhitehouse.archives.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf); see also FEDERAL TRADE COMMISSION (F.T.C), *Big Data: A Tool for Inclusion or Exclusion?* (Jan. 2016), <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

<sup>9</sup> Barbara Ortutay, *Facebook to overhaul ad targeting to prevent discrimination*, ASSOCIATED PRESS, March 19, 2019, <https://www.apnews.com/38c0dbd8acb14e3fbc7911ea18fafd58>.

<sup>10</sup> 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),

advertisers to select which zip codes to include or exclude from receiving an ad, and draw a red line on a map showing the excluded neighborhoods.<sup>11</sup> Academic research suggests that Meta also used ad delivery algorithms that reproduce discrimination even when the advertiser did not intend to discriminate, including again in the housing, credit services, and employment contexts.<sup>12</sup> Similar practices have been the target of investigations, including at Twitter and Google.<sup>13</sup>

Retail websites have been found to charge different prices based on the demographics of the user.<sup>14</sup> For example, an online shopper's distance from a physical store, as well as distance from the store's competitors, has been used in algorithms setting online prices, resulting in price discrimination. Because of historical redlining and segregation, and the lack of retail options in many low-income neighborhoods, this resulted in low-income communities of color paying higher prices than wealthier, whiter neighborhoods when they shop online.

In housing, algorithmic tools that are used to identify prospective home loan applicants or tenants can cement and reflect centuries of discrimination. For instance, 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.<sup>15</sup> In fact, Black applicants with less debt than white applicants are still more likely to be rejected for a mortgage. Similarly, in 2023, reporters discovered that the algorithmic scoring system used by

---

<https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/>.

<sup>11</sup> “[Facebook] has provided a toggle button that enables advertisers to exclude men or women from seeing an ad, a search-box to exclude people who do not speak a specific language from seeing an ad, and a map tool to exclude people who live in a specified area from seeing an ad by drawing a red line around that area.” Charge of Discrimination, *U.S. Dept. of Hous. and Urban Dev. v. Facebook, Inc.*, FHEO No. 01-18-0323-8 at 4 (Mar. 28, 2019),

[https://www.hud.gov/sites/dfiles/Main/documents/HUD\\_v\\_Facebook.pdf](https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf); 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, *Liapes v. Facebook*, No. 30-CIV-01712, at 10 (Calif. Super. Ct. 2021), <https://lawyerscommittee.org/wp-content/uploads/2021/03/Leave-and-Amicus-Combined.pdf>.

<sup>12</sup> 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/>.

<sup>13</sup> *Id.*

<sup>14</sup> 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>; Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, HARV. BUS. REVIEW (Nov. 8, 2019), <https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias>.

<sup>15</sup> 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>.



the Los Angeles Homeless Services Authority discriminated against Black and Latino people, giving white applicants higher priority in the agency's housing system.<sup>16</sup>

Discrimination in the insurance market is also common. Scoring algorithms used by auto insurers judge applicants "less on driving habits and increasingly on socioeconomic factors,"<sup>17</sup> resulting in higher rates and fewer options for residents of majority Black neighborhoods.<sup>18</sup> These disparities are so significant that, in some instances, insurers charge rates more than 30 percent higher in Black and Brown neighborhoods, regardless of neighborhood affluence.<sup>19</sup> In another case, 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,<sup>20</sup> contributing to discriminatory higher premiums routinely paid by consumers of color who often lack competitive options for insurance. Despite these concerns, the Allstate personalized pricing algorithm was still implemented in other states.<sup>21</sup>

Similarly, algorithmic tools used in consumer financial markets often determine who can access a loan or credit based on a consumer's identity.<sup>22</sup> 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

---

<sup>16</sup> Colin Lecher & Maddy Venrer, *Black and Latino Homeless People Rank Lower on L.A.'s Housing Priority List*, L.A. TIMES (Feb. 28, 2023), <https://www.latimes.com/california/story/2023-02-28/black-latino-homeless-people-housing-priority-list-los-angeles>.

<sup>17</sup> CONSUMER REPS., *The Truth About Car Insurance* (July 30, 2015),

<https://www.consumerreports.org/cro/car-insurance/auto-insurance-special-report/index.htm>.

<sup>18</sup> 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/>.

<sup>19</sup> 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>.

<sup>20</sup> Maddy Varner & Aaron Sankin, *Suckers List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders*, THE MARKUP (Feb. 25, 2020), <https://themarkup.org/allstates-algorithm/2020/02/25/car-insurance-suckers-list>.

<sup>21</sup> See Aaron Sankin, *Michigan Regulators Question Allstate's Car Insurance Pricing*, THE MARKUP (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>.

<sup>22</sup> 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>.



70 percent of white applicants.<sup>23</sup> Even when consumers of color are able to access financial services, they are often charged higher rates as a result of “algorithmic strategic pricing.” One study found that the use of such tools resulted in Black and Latino borrowers paying higher interest rates on home purchase and refinance loans when compared to similar white borrowers. The difference alone costs Black and Latino customers \$250 to \$500 million every year.<sup>24</sup>

These harms occur primarily in three ways. First, a company holding personal data uses them to directly discriminate against people of color or other marginalized groups; second, a company holding personal data makes them available to other actors who use them to discriminate; or third, a company designs its data processing practices in a manner that negligently, recklessly, or knowingly causes discriminatory or otherwise harmful results—*e.g.*, algorithmic bias or promotion of disinformation. But 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.<sup>25</sup>

The common denominator in these examples is the sloppy or abusive use of personal data and algorithmic tools. By prohibiting algorithmic discrimination, mandating data minimization and other privacy protections, and requiring companies to test and prove that their algorithms are safe and effective, many harms can be prevented or mitigated.

#### **IV. Consumers Cannot Reasonably Avoid the Harms from Opaque, Discriminatory Algorithms; The Act of Avoidance is Itself Harmful.**

---

<sup>23</sup> 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>.

<sup>24</sup> Laura Counts, *Minority homebuyers face widespread statistical lending discrimination, study finds*, UNIV. OF CALIF. BERKELEY HAAS SCH. OF BUS. (Nov. 13, 2018), <https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/>.

<sup>25</sup> See Valerie Schneider, *Locked Out by Big Data: How Big Data, Algorithms and Machine Learning May Undermine Housing Justice*, 52.1 Colum. Hum. Rts. L. Rev. 251, 254 (2020), [https://blogs.law.columbia.edu/hrlr/files/2020/11/251\\_Schneider.pdf](https://blogs.law.columbia.edu/hrlr/files/2020/11/251_Schneider.pdf); James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 Fordham Urb. L.J. 219, 229 (2019); Mathias Risse, *Human Rights and Artificial Intelligence: An Urgently Needed Agenda*, 41 Hum. Rts. Q. 1, 11 (2019); EXEC. OFF. OF THE PRESIDENT, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* 1, 5 (2016), [https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016\\_0504\\_data\\_discrimination.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf).

Consumers are unable to avoid the risk of substantial injury posed by algorithmic systems because their operations are opaque to consumers. Although algorithmic discrimination is widespread, many consumers who are harmed are often unaware that they have been impacted by an algorithm in the first place. Even when consumers are aware that they may have been affected by an algorithm, there is often little transparency about how an algorithm made a decision about a given opportunity or service. Low-income consumers, in particular, may lack the resources or opportunities to fight or avoid exploitative practices or products. It is unrealistic and unfair to expect consumers to avoid algorithmic systems when they do not know they have been subjected to it or how the decision affected them.

Due to the “black box” nature of many algorithmic systems, consumers cannot reasonably avoid the harms of discrimination. As FTC leaders have noted in recent enforcement actions, business practices that cause substantial injury to consumers on the basis of immutable characteristics such as race are not reasonably avoidably and are not outweighed by countervailing benefits.<sup>26</sup> The FTC’s actions to combat discrimination with consumer protection law are well-grounded in decades of civil rights case law. Unfair and deceptive practices statutes have a long history in the struggle for civil rights. For example, such a provision in the Interstate Commerce Act was used to desegregate bus terminals and railroads, including the Supreme Court’s landmark 1960 decision in *Boynton v. Virginia* that catalyzed the Freedom Rides.<sup>27</sup>

Discrimination in this context is not a product feature touted on a box and weighed in the aisle of a marketplace. In the context of algorithmic systems, consumers typically have no way of knowing what factors a firm uses to make decisions about the opportunities, products, or services offered to the consumer and no way to discern which firms are discriminating and which are not. Moreover, there often are intermediary firms, service providers, or other third parties in between the consumer and the opportunity—such as advertising networks or assessment tools for prospective employees—and those intermediaries may engage in discrimination.

---

<sup>26</sup> See *F.T.C., Joint Statement of Chair Lina M. Khan, Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro M. Bedoya In the Matter of Passport Auto. Grp., F.T.C. File No. 202 3199, at 3* (Oct. 18, 2022) (auto sales), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/joint-statement-of-chair-lina-m.-khan-commissioner-rebecca-kelly-slaughter-and-commissioner-alvaro-m.-bedoya-in-the-matter-of-passport-auto-group.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/joint-statement-of-chair-lina-m.-khan-commissioner-rebecca-kelly-slaughter-and-commissioner-alvaro-m.-bedoya-in-the-matter-of-passport-auto-group.pdf). In the past, the F.T.C. has also addressed deceptive advertisements related to housing discrimination. See *In re E.G. Reinsch, Inc.*, 75 F.T.C. 210 (1969); *In re First Buckingham Cmty., Inc.*, 73 F.T.C. 938 (1968).

<sup>27</sup> See *Boynton*, 364 U.S. 454 (1960) (bus terminal segregation); *Henderson v. United States*, 339 U.S. 816 (1950) (dining car segregation); *Mitchell v. United States*, 313 U.S. 80 (1941) (railcar segregation); *Keys v. Carolina Coach Co.*, 64 M.C.C. 769 (Interstate Commerce Commission 1955) (bus segregation). See also *Orloff v. F.C.C.*, 352 F.3d 415, 420 (D.C. Cir. 2003) (Communications Act of 1934 prohibits race and income discrimination as unjust and unreasonable practices).

But even if a consumer knows that an algorithm discriminates against them, they may be unable to avoid using it. For example, someone seeking housing, employment, insurance, or credit may have no choice but to submit to an automated decision-making tool even if they know it is unfair.<sup>28</sup> Or due to market concentration, a consumer may have little or no access to online services without subjecting themselves to discrimination. The FTC recently analyzed the data practices of the six largest internet service providers and found that many “allo[w] advertisers to target consumers by their race, ethnicity, sexual orientation, economic status, political affiliations, or religious beliefs.”<sup>29</sup>

When a firm imposes a greater burden on some people to access opportunities because of their protected characteristics, the additional time, money, effort, or humiliation to overcome that hurdle is an injury.<sup>30</sup> The “imposition of a barrier” creates “the inability to compete on equal footing.”<sup>31</sup> Thus, even if alternative services are available—and they are equal—it is inherently unjust and unfair to require consumers to avoid the harm. An individual cannot reasonably avoid discrimination because the very act of avoidance itself is a form of segregation that causes a substantial injury.

This is why the Biden-Harris Administration has already taken a series of actions to mitigate the risks of AI, including by outlining key principles for advancing civil rights and equity in the Blueprint for an AI Bill of Rights,<sup>32</sup> Executive Order 14091 (“Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government”),<sup>33</sup> Executive Order 14110 (“Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”),<sup>34</sup> and the Office of Management and Budget’s proposed memorandum on agency use of AI.<sup>35</sup> Together, these actions direct agencies across the federal government to use their existing authorities to prevent and remedy algorithmic discrimination. While these measures are crucial for protecting consumers from the harms of discriminatory algorithms, it is now time for Congress to take the next step and enact legislation.

---

<sup>28</sup> See *supra* § III.

<sup>29</sup> F.T.C., *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* iii (Oct. 21, 2021), [https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402\\_isp\\_6b\\_staff\\_report.pdf](https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf).

<sup>30</sup> See, e.g., *Heckler*, 465 U.S. at 740.

<sup>31</sup> *Ne. Fla. Chapter of Ass’n Gen. Contractors of Am. v. City of Jacksonville, Fla.*, 508 U.S. 656, 666 (1993).

<sup>32</sup> *Blueprint*.

<sup>33</sup> Exec. Order No. 14091, 88 Fed. Reg. 10825 (Feb. 16, 2023).

<sup>34</sup> Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

<sup>35</sup> OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, Proposed Memorandum, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Nov. 1, 2023), <https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf>.

## V. Solutions

The persistence and proliferation of such discriminatory conduct highlights the need for further action. To address these harms, Congress should enact legislation regulating the use of algorithmic technologies that prioritizes civil rights and consumer protections. It should include the following six core principles for ensuring that algorithmic systems and related data practices are safe, effective, and fair.

*First*, AI regulation must seriously address algorithmic bias and discrimination through bright line rules and effective examination of the technology deployed. Legislation should include specific anti-discrimination provisions to prohibit algorithmic discrimination, including disparate impact. These should include narrow but reasonable exceptions for self-testing to prevent or mitigate bias and for diversifying a consumer pool through outreach to underserved communities. The anti-discrimination provision from the bipartisan American Data Privacy and Protection Act, which passed out of the U.S. House Energy & Commerce Committee last year on a 53-2 vote, is a good model.<sup>36</sup>

*Second*, AI should be evaluated and assessed, both *before* and *after* deployment, for discrimination, bias, and other harms. 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.<sup>37</sup> Reviewing algorithms in both the design and deployment phases proactively detects and prevents harm and promotes responsible innovation.

*Third*, Developers and deployers of AI should have a duty of care requiring that the products they offer are safe and effective and be liable if they aren't. An algorithm is safe if it is evaluated by a pre-deployment assessment, reasonable steps are taken to prevent it from causing harm, and its use is not unfair or deceptive. An algorithm is effective if it functions as expected, intended, and publicly advertised. Legislation should also prohibit a developer or deployer from engaging in deceptive marketing, off-label uses, and abnormally dangerous activities. Establishing a duty

---

<sup>36</sup> See American Data Privacy and Protection Act ("ADPPA"), H.R. 8152, 117th Cong. § 207(a) (2022), <https://www.congress.gov/bill/117th-congress/house-bill/8152/text/rh>.

<sup>37</sup> See Louis D. Brandeis, *What Publicity Can Do*, Harper's Weekly (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.").

of care ensures that companies must take adequate steps to protect consumers and make sure that their products work as intended.

*Fourth*, AI regulation should include transparency and explainability requirements so that consumers know when, how, and why a company is using AI and how it affects them. Companies must provide individuals with easy-to-understand notices about whether and how an algorithmic system affects their rights. A regulator should be empowered to write rules for when and how a company needs to provide individualized explanations and rights to appeal decisions informed by AI. Companies also need to publish annual reports about their impact assessments and data practices. Without public transparency, individuals cannot make informed decisions about how they interact with algorithmic systems and are unable to seek redress when harm occurs.

*Fifth*, there should be data protection requirements, so that AI is not trained on the data of people who have not consented to it and to safeguard consumer's privacy. Training and testing AI to make it fair and unbiased requires not just a lot of personal data, but a lot of highly sensitive personal data, like race and sex information. For consumers to be willing to share that information, they need to be able to trust that it will not be misused for secondary purposes and that will be kept secure. Developers and deployers should be required to collect and use only as much personal data as is reasonably necessary and proportionate to provide the services that consumers expect, and to safeguard that data. Developers should have an additional requirement to get affirmative express consent to use personal data to train algorithms. Individuals also should be able to access, correct, and delete their personal data. These data protection requirements are necessary to enable individuals to safely share their sensitive personal information without fear.

*Sixth*, legislation should establish robust oversight and multiple levels of enforcement. This must include a private right of action. Individuals need to be able to vindicate their own rights in court because, historically, Black people and other people of color could not rely on government agencies to defend their rights. There should also be enforcement by state attorneys general and a federal agency. The federal agency needs regulatory authority as well to effectively regulate and mandate compliance with technical aspects of AI regulation, like auditing and transparency. Purveyors of algorithmic systems infringing people's rights should not be immune from liability.

## **VI. Conclusion**

While the threats of AI are often described as matters of futuristic science fiction, algorithmic tools are already harming Black people and other communities of color every day. As Vice President Kamala Harris recently warned about growing concern that AI could pose an existential threat to humanity, "There are additional

threats that also demand our action—threats that are currently causing harm and which, to many people, also feel existential.”<sup>38</sup> Congress must act because otherwise communities of color will keep bearing these burdens. By implementing bright-line rules and guardrails on the development and deployment of algorithmic systems, Congress can unlock this technology’s potential to expand opportunities and level the playing field. We appreciate this Committee’s attention to this important issue and look forward to working with the Committee to advance civil rights and consumer protections for AI.

---

<sup>38</sup> SPEECHES AND REMARKS, WHITE HOUSE, *Remarks by Vice President Harris on the Future of Artificial Intelligence | London, United Kingdom* (Nov. 1, 2023), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/11/01/remarks-by-vice-president-harris-on-the-future-of-artificial-intelligence-london-united-kingdom/>.

## **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 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.

### **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.”<sup>1</sup> Lenders used formulas mandated by Fannie Mae and Freddie Mac, which were known to be detrimental to people of color.<sup>2</sup>
- 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 literal redlining.<sup>3</sup> Meta agreed to

---

<sup>1</sup> 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>.

<sup>2</sup> *Id.*

<sup>3</sup> 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-



create a new system to reduce disparities in the delivery of housing ads as part of the settlement.<sup>4</sup> Facebook has also been sued by civil rights advocates for similar conduct and causes of action.<sup>5</sup>

- 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 promises to address the problem.<sup>6</sup> Facebook’s own civil rights auditors called out the risk of algorithmic bias in its advertising system.<sup>7</sup>
- Google and Twitter have both been investigated by HUD for similarly discriminating in housing advertisements in violation of the Fair Housing Act.<sup>8</sup>

---

CIV-01712 (Cal. Super. Ct. Mar. 5, 2021), <https://lawyerscommittee.org/wp-content/uploads/2021/03/Leave-and-Amicus-Combined.pdf>.

<sup>4</sup> 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>.

<sup>5</sup> 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>.

<sup>6</sup> **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/>.

<sup>7</sup> 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>.

<sup>8</sup> 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),

- Landlords and other housing providers use social media targeted advertising tools to engage in discrimination on the basis of race, sex, and age.<sup>9</sup>
- Landlords use tenant screening and background check algorithmic systems that frequently produce flawed reports that cause denials of lease applications.<sup>10</sup> These oversimplified recommendation systems disproportionately impact Black and Latino tenants, making it harder for them to secure affordable housing.<sup>11</sup> The DOJ has said that tenant screening and risk scoring algorithms are subject to the Fair Housing Act.<sup>12</sup>
- 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.<sup>13</sup>
- Some of the largest property managers in the country use property management 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.<sup>14</sup>

---

<https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/>.

<sup>9</sup> 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>.

<sup>10</sup> 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>.

<sup>11</sup> 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/>.

<sup>12</sup> 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/>.

<sup>13</sup> 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>.

<sup>14</sup> 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>.

- 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.<sup>15</sup>
- 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.<sup>16</sup>

## 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.”<sup>17</sup>
- Automated tools—including those using facial recognition or facial analysis—are increasingly a prevalent and pervasive part of the hiring process, but there are serious concerns that these systems are racially biased and there is little transparency to verify their safety or efficacy.<sup>18</sup>

---

<sup>15</sup> 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>.

<sup>16</sup> 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>.

<sup>17</sup> Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn, at 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>.

<sup>18</sup> 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>.

- 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.<sup>19</sup>
- Amazon previously used a machine learning tool to assess job applicants for technical positions, but it systematically discriminated in favor of men.<sup>20</sup>
- Algorithms are becoming more common tools to aid human resources departments for recruitment and development, but there are concerns that these tools can contribute to discrimination.<sup>21</sup> These “bossware” tools are being sold to government agencies as well.<sup>22</sup>
- Employee surveillance tools deployed during the pandemic to monitor remote workers are very invasive and likely to persist beyond the pandemic.<sup>23</sup> 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.”<sup>24</sup>
- Digital identity credentialing 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.”<sup>25</sup>

---

<sup>19</sup> 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/>.

<sup>20</sup> 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-insight/idUSKCN1MK08G>.

<sup>21</sup> 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. Res. 795 (2020), <https://doi.org/10.1007/s40685-020-00134-w>.

<sup>22</sup> 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>.

<sup>23</sup> 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/>.

<sup>24</sup> *Id.*

<sup>25</sup> 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/>.

- 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.<sup>26</sup>

## Credit and finance

- 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.<sup>27</sup>
- 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.<sup>28</sup>
- 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.<sup>29</sup>
- Lax data security at credit reporting agencies such as Experian<sup>30</sup> and Equifax<sup>31</sup> have resulted in breaches exposing the sensitive credit data of millions of Americans. As the FTC has found, identity theft and fraud disproportionately impact communities of color and low-income consumers are also less likely to have the resources to bounce back after experiencing fraud.<sup>32</sup>

---

<sup>26</sup> 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/>.

<sup>27</sup> 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](https://www.nber.org/system/files/working_papers/w25943/w25943.pdf).

<sup>28</sup> 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/>.

<sup>29</sup> 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>.

<sup>30</sup> 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/>.

<sup>31</sup> 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>.

<sup>32</sup> 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->



- 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.”<sup>33</sup>
- 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.<sup>34</sup> After reporters discovered that Facebook targeted ads for financial services based on age, the company pledged to remove the discriminatory content.<sup>35</sup>
- Data used to score consumers’ credit has been shown to be capable of predicting the race and gender of loan applicants.<sup>36</sup>
- 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 learning algorithm to overestimate women applicants’ default rate. Including gender data reduced the algorithm’s gender discrimination by 2.8 times.<sup>37</sup>

## 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

---

[color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report oct 2021-508-v2.pdf](https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/); 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/](https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/).

<sup>33</sup> Aaron Reike & Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, Upturn 15 (Oct. 2015), <https://www.upturn.org/reports/2015/led-astray/>.

<sup>34</sup> 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>.

<sup>35</sup> 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>.

<sup>36</sup> 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>.

<sup>37</sup> 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>.

street these days . . . You're going to get lumped in with a lot of bad things.”<sup>38</sup> All forms of insurance are now “adjusting premiums and policies based on new forms of surveillance.”<sup>39</sup>

- 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.<sup>40</sup> Insurance premiums are set by actuarial algorithms using many non-driving factors, which contributes to higher rates in Black neighborhoods and for individuals with less education or lower-paying jobs.<sup>41</sup> These scoring algorithms judge applicants “less on driving habits and increasingly on socioeconomic factors.”<sup>42</sup>
- 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,<sup>43</sup> 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.<sup>44</sup>
- 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

---

<sup>38</sup> 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>.

<sup>39</sup> 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>.

<sup>40</sup> 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>.

<sup>41</sup> 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/>.

<sup>42</sup> Consumer Reps., *The Truth About Car Insurance* (July 30, 2015), <https://www.consumerreports.org/cro/car-insurance/auto-insurance-special-report/index.htm>.

<sup>43</sup> 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>.

<sup>44</sup> 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>.



as driver name, driver fatigue, driver heartrate, and the language used on a dashboard display.<sup>45</sup> Companies use this data in usage-based insurance, which charges higher premiums to “risky drivers.”<sup>46</sup> These types of 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.<sup>47</sup> 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.

## Public health and healthcare

- Social media news feed algorithms and advertising systems significantly contributed to the amplification of health disinformation about COVID-19.<sup>48</sup> 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 Organisation (WHO) and the Centers for Disease Control and Prevention (CDC).”<sup>49</sup> Public health agencies have faced particular difficulties getting their paid public service announcements to reach Black social media users.<sup>50</sup> This disparity in reach has real-life consequences, as COVID disproportionately harms Black and Hispanic Americans, who experience higher disease

---

<sup>45</sup> 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).

<sup>46</sup> Keegan & Ng, *supra* note 45.

<sup>47</sup> 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/>.

<sup>48</sup> *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>.

<sup>49</sup> Avaaz, *Facebook’s Algorithm: A Major Threat to Public Health* (Aug. 19, 2020), [https://secure.avaaz.org/campaign/en/facebook\\_threat\\_health/](https://secure.avaaz.org/campaign/en/facebook_threat_health/).

<sup>50</sup> *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>.

prevalence, hospitalization, and mortality compared to whites and who have less access to healthcare as a consequence of systemic racism.<sup>51</sup>

- 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.”<sup>52</sup>
- A widely used algorithm for identifying health needs of patients was 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.<sup>53</sup> Another algorithm made “wildly irrational” decisions depriving necessary care to people with disabilities.<sup>54</sup>
- 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 user engagement.<sup>55</sup> 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.”<sup>56</sup> 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.<sup>57</sup> When teens engaged in suicidal ideation, 6% of them traced it to Instagram.<sup>58</sup> 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

---

<sup>51</sup> 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/>.

<sup>52</sup> 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>.

<sup>53</sup> 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 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/>.

<sup>54</sup> 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>.

<sup>55</sup> 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>.

<sup>56</sup> *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/>.

<sup>57</sup> Wells et al., *supra* note 55.

<sup>58</sup> *Id.*

eating disorder content within minutes once the accounts viewed and liked content related to body image, eating disorders, and mental health.<sup>59</sup>

- 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.”<sup>60</sup> People of color are less likely to have access to specialty medical care,<sup>61</sup> 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.<sup>62</sup> There is significant concern that data collected by Google and other entities, especially location data, could be used to prosecute people seeking reproductive healthcare.<sup>63</sup> 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.<sup>64</sup> 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,<sup>65</sup> testing showed that searches for directions and routes taken to abortion clinics, and other data, like abortion-related search engine history, can remain

---

<sup>59</sup> 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](https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf).

<sup>60</sup> 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-abortion/>.

<sup>61</sup> 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.”).

<sup>62</sup> 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>.

<sup>63</sup> 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-abortion-00045906>.

<sup>64</sup> See Katherine Kortzmit 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](https://www.guttmacher.org/sites/default/files/report_pdf/characteristics-us-abortion-patients-2014.pdf).

<sup>65</sup> 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/>.

visible on users' activity pages for months after being logged.<sup>66</sup> Google has a notable history of collecting location data against users' wishes.<sup>67</sup>

- 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.<sup>68</sup> Facebook has collected sensitive patient information from healthcare and hospital websites, including data on people seeking abortions and children.<sup>69</sup> It collected health information, including ovulation data, from health apps without user consent.<sup>70</sup>
- 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.<sup>71</sup> 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.<sup>72</sup>

---

<sup>66</sup> 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*, Washington Post (May 9, 2023), <https://www.washingtonpost.com/technology/2023/05/09/google-privacy-abortion-data/>.

<sup>67</sup> 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>.

<sup>68</sup> 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>.

<sup>69</sup> 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>.

<sup>70</sup> 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>.

<sup>71</sup> Gioacchino Tangari et al., *Mobile Health and Privacy: Cross Sectional Study*, BMJ (June 17, 2021), <https://www.bmj.com/content/373/bmj.n1248>.

<sup>72</sup> 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>.

- Data brokers also sell personal data to health care providers, including “criminal records, online purchasing histories, retail loyalty programs and voter registration data.”<sup>73</sup> These data can be fed into algorithms used to classify patients’ health risks and can produce biases if not handled correctly.<sup>74</sup> 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.<sup>75</sup>
- 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, and thus are only half as accurate when diagnosing Black patients.<sup>76</sup> 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.<sup>77</sup>

## 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.<sup>78</sup>
- 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.<sup>79</sup>

---

<sup>73</sup> 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>.

<sup>74</sup> See Obermeyer, *supra* note 53.

<sup>75</sup> 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/>.

<sup>76</sup> 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>.

<sup>77</sup> 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>.

<sup>78</sup> 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>.

<sup>79</sup> 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>.



- Higher education institutions are increasingly adopting “student success analytics” intended to aid students in their studies.<sup>80</sup> 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 will be steered away from pursuing math and science.<sup>81</sup> Black students were deemed “higher risk for failure” as much as four times as often as white peers.<sup>82</sup>
- 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.<sup>83</sup> Enrollment algorithms often discriminate against people of color and women.<sup>84</sup> 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.<sup>85</sup> More than 75 percent of colleges and universities use analytics in enrollment management and admissions decisions.<sup>86</sup>
- 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.<sup>87</sup>

---

<sup>80</sup> 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>.

<sup>81</sup> 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>.

<sup>82</sup> *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).

<sup>83</sup> 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/>.

<sup>84</sup> See *id.*

<sup>85</sup> 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/>.

<sup>86</sup> Ronald Yanosky & Pam Arroya, *The Analytics Landscape of Higher Education, 2015*, EDUCAUSE, at 17 (2015) <https://library.educause.edu/~media/files/library/2015/5/ers1504cl.pdf>.

<sup>87</sup> 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.<sup>88</sup> 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.”<sup>89</sup> “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.”<sup>90</sup>
- 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.<sup>91</sup> 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.<sup>92</sup>
- 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.<sup>93</sup> Similarly, “aggression detector” software marketed to schools to monitor students by recording audio and monitoring for “threats” often fail to identify or misidentify sounds.<sup>94</sup> 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

---

<sup>88</sup> 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>.

<sup>89</sup> 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/>.

<sup>90</sup> *Id.*

<sup>91</sup> 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>.

<sup>92</sup> 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-a2j3vsvtjhhjj36n57ri5zdhi-story.html>.

<sup>93</sup> 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>.

<sup>94</sup> 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/>.



messages, photos, app data, location data, and other communications.<sup>95</sup> Other schools have used AI-driven software to surveil students' social media for warning signs of violence, without the students' permission or awareness.<sup>96</sup>

- 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.<sup>97</sup> Black women, in particular, are at greater risk of being falsely accused of cheating by these automated tools.<sup>98</sup>

## 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.<sup>99</sup>
- 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.<sup>100</sup>
- Uber enabled drivers to discriminate against passengers with what were perceived to be Black names and provide more expensive services to women passengers.<sup>101</sup>

---

<sup>95</sup> 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>.

<sup>96</sup> 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>.

<sup>97</sup> 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>.

<sup>98</sup> 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>.

<sup>99</sup> 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/>.

<sup>100</sup> 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. of Youth & Adolescence 245, 255 (Oct. 2023), <https://link.springer.com/article/10.1007/s10964-022-01689-z>.

<sup>101</sup> 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>.

- 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.<sup>102</sup> 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 marketers attempting to reach young Black, Latinx, and Asian people with products and services relating to other aspects of their lives.”<sup>103</sup>
- 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.<sup>104</sup>
- “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.<sup>105</sup>
- 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

---

<sup>102</sup> 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>.

<sup>103</sup> 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>.

<sup>104</sup> See Kevin Collier, *Twitter’s Racist Algorithm Is Also Ageist, Ableist and Islamophobic, Researchers Find*, NBC News (Aug. 9, 2021), <https://www.nbcnews.com/tech/tech-news/twitters-racist-algorithm-also-ageist-ableist-islamophobic-researchers-rcna1632>.

<sup>105</sup> See *Serving Communities of Color*, *supra* note 32, 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/>.

executives received those data, they halted further research into racial bias in the system.<sup>106</sup>

- 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.<sup>107</sup> For example, algorithms that distribute discount-related ads tend to direct those ads toward high-income white users.<sup>108</sup>
- 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.<sup>109</sup>
- Leading automated speech recognition software from Amazon, Apple, Google, IBM, and Microsoft are all less accurate when processing the speech of Black Americans.<sup>110</sup>
- Black influencers drive popular trends on TikTok but do not equitably share in the profits created by their monetized content.<sup>111</sup>
- 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.<sup>112</sup> 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.<sup>113</sup>

---

<sup>106</sup> 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>.

<sup>107</sup> 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>.

<sup>108</sup> Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, Harv. Bus. Review (Nov. 8, 2019), <https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias>.

<sup>109</sup> 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/>.

<sup>110</sup> Allison Koenecke et al., *Racial disparities in automated speech recognition*, 117 PNAS 7684 (2020), <https://www.pnas.org/doi/10.1073/pnas.1915768117>.

<sup>111</sup> 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>.

<sup>112</sup> 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/>.

<sup>113</sup> 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/>.

## Online hate, harassment, and threats

- 52% of U.S. adults reported personally experiencing online harassment, largely through social media.<sup>114</sup> 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.<sup>115</sup> 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.<sup>116</sup> 58% of all teens have experience online harassment and 39% report experiences of severe harassment.<sup>117</sup> 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.<sup>118</sup>
- Online dating carries greater risks for people of color and LGBTQ 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 compared to straight daters. Overall, White users were more likely to say they felt safe dating online than Black, Hispanic and Asian adults.”<sup>119</sup>
- 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.<sup>120</sup> For 20%, online threats turned into offline attacks or abuse. Disinformation narratives fuel misogynistic attacks.<sup>121</sup> 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%).<sup>122</sup> “Attacking women journalists is a fast, easy way to generate

---

<sup>114</sup> 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-Harassment-2023\\_0.pdf](https://www.adl.org/sites/default/files/pdfs/2023-06/Online-Hate-and-Harassment-2023_0.pdf).

<sup>115</sup> *Id.* at 32.

<sup>116</sup> *Id.* at 15, 35.

<sup>117</sup> *Id.* at 44.

<sup>118</sup> 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).

<sup>119</sup> 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/>.

<sup>120</sup> 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](https://www.icfj.org/sites/default/files/2022-11/ICFJ_UNESCO_The%20Chilling_2022_1.pdf).

<sup>121</sup> *Id.* at 23, 32, 85.

<sup>122</sup> *Id.* at 47–48.

engagement on social media, experts say. Platforms reward outrage.”<sup>123</sup> “Many who are targeted report on the internet itself and how it is being used to bolster extremists.”<sup>124</sup>

- Platform algorithms help white supremacists connect with each other and systematically promote divisive material in the pursuit of maximizing user engagement.<sup>125</sup> 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.”<sup>126</sup> 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.”<sup>127</sup> When these issues were raised to Facebook executives, they declined to make changes.<sup>128</sup>
- YouTube video recommendations systematically recommend harmful and progressively more extreme content to viewers, creating pathways to white supremacy and hate group recruitment.<sup>129</sup>
- Following the murder of George Floyd by Minneapolis police, racist disinformation about his death surged on Facebook, YouTube, and Twitter.<sup>130</sup>
- 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

---

<sup>123</sup> 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/>.

<sup>124</sup> *Id.*

<sup>125</sup> 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.”).

<sup>126</sup> 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](https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499?mod=hp_lead_pos5).

<sup>127</sup> *Id.*

<sup>128</sup> *See id.*

<sup>129</sup> 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, at 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](https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf)

<sup>130</sup> 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>.



Americans tripling on the platform.<sup>131</sup> 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.<sup>132</sup>

- Large language models and other AI trained on real-world data sets capture and reproduce racist stereotypes and biases.<sup>133</sup> Hateful autocomplete recommendations in Google Search are a highly visible manifestation of this problem.<sup>134</sup> As is Google’s photo-categorization software labeling Black people as gorillas, which Google failed to fix for years.<sup>135</sup> 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.<sup>136</sup>

---

<sup>131</sup> 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-voel-roth/>.

<sup>132</sup> 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/>.

<sup>133</sup> 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>.

<sup>134</sup> Issie Lapowsky, *Google Autocomplete Still Makes Vile Suggestions*, WIRED (Feb. 12, 2018), <https://www.wired.com/story/google-autocomplete-vile-suggestions/>.

<sup>135</sup> 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/>.

<sup>136</sup> 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>.

- 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.<sup>137</sup>
- Facebook profits from running ads on searches for hate group pages.<sup>138</sup> Google’s ad network has been manipulated to help monetize websites that promote violence and misinformation.<sup>139</sup> Both have previously allowed ad targeting based on racism and hate speech.<sup>140</sup>
- Commercial surveillance tools are used by domestic abusers and stalkers to track, threaten, and harm their targets.<sup>141</sup>
- 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.<sup>142</sup>
- Facebook was instrumental in enabling the genocide of Rohingya Muslims in Myanmar.<sup>143</sup>

---

<sup>137</sup> 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-lambda-racist-2022-7>.

<sup>138</sup> 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/>.

<sup>139</sup> 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>.

<sup>140</sup> 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>.

<sup>141</sup> Sarah Jeong, *Surveillance Begins at Home*, Forbes: Tech (Oct. 28, 2014), <https://www.forbes.com/sites/sarahjeong/2014/10/28/surveillance-begins-at-home/>.

<sup>142</sup> 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-05889f1f4076709c47fc9a18dbec818a>.

<sup>143</sup> 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>;



- 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.<sup>144</sup>
- Facebook allowed ads to run in Kenya that promoted ethnic cleansing in the run-up to a national election.<sup>145</sup>
- 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.<sup>146</sup>
- 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.<sup>147</sup>
- 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.<sup>148</sup>

### **Voter intimidation and election disinformation**

- 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.<sup>149</sup> They spent only \$1,000 on

---

<sup>144</sup> 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>.

<sup>145</sup> 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>.

<sup>146</sup> 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>.

<sup>147</sup> Rhys Leahy et al., *Connectivity Between Russian Information Sources and Extremist Communities Across Social Media Platforms*, 4 *Frontiers Pol. Sci.*, June 22, 2022, at 6, <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>.

<sup>148</sup> 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>.

<sup>149</sup> See *Nat’l Coal. on Black Civic Participation v. Wohl*, 498 F. Supp. 3d 457 (S.D.N.Y. 2020).

the robocalls.<sup>150</sup> The court ruled this conduct violated the Voting Rights Act and the Ku Klux Klan Act of 1871.<sup>151</sup> 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.<sup>152</sup>

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.”<sup>153</sup>

- 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.”<sup>154</sup> 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.”<sup>155</sup>

---

<sup>150</sup> 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.

<sup>151</sup> *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).

<sup>152</sup> *Nat’l Coal. on Black Civic Participation*, 498 F. Supp. 3d at 464.

<sup>153</sup> *Nat’l Coal. on Black Civic Participation*, 2023 WL 2403012, at \*22.

<sup>154</sup> 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>.

<sup>155</sup> 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),

- 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.<sup>156</sup> The campaign also used racially divisive issues in targeted ads.<sup>157</sup> Foreign adversaries used conventional advertising and targeting tools on social media,<sup>158</sup> showing the dangerous ways in which off-the-shelf targeted advertising tools can be abused.<sup>159</sup> 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.<sup>160</sup>
- Social media plays a key role in disinformation campaigns that spread conspiracy theories and seek to undermine election integrity.<sup>161</sup> 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.<sup>162</sup> 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.<sup>163</sup> “[T]o tackle thorny issues like misinformation, [Facebook

---

<https://www.justice.gov/usao-edny/pr/social-media-influencer-douglass-mackey-convicted-election-interference-2016>.

<sup>156</sup> 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*, at 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.”).

<sup>157</sup> 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/>.

<sup>158</sup> 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>.

<sup>159</sup> 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>.

<sup>160</sup> 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>.

<sup>161</sup> See Election Integrity P’ship, *The Long Fuse: Misinformation and the 2020 Election* (2021), <https://www.eipartnership.net/report>.

<sup>162</sup> 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>.

<sup>163</sup> 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>.

employees] often had to demonstrate that their proposed solutions wouldn't anger powerful partisans or come at the expense of Facebook's growth."<sup>164</sup>

- YouTube was more likely to recommend videos involving election fraud conspiracy theories to users known to be skeptical about election validity, amplifying fringe disinformation.<sup>165</sup> Its AI content moderation system struggled with combatting disinformation in the short-form YouTube Shorts and in Spanish language videos.<sup>166</sup>
- The proliferation of disinformation on social media was a major contributor to false narratives and conspiracy theories attacking the outcome of the 2020 election,<sup>167</sup> culminating in the violent attack on the U.S. Capitol on January 6, 2021.<sup>168</sup> 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.<sup>169</sup> 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.<sup>170</sup>
- 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

---

<sup>164</sup> 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>.

<sup>165</sup> 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>.

<sup>166</sup> 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>.

<sup>167</sup> 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/>.

<sup>168</sup> See generally Ryan Goodman & Justin Hendrix, *January 6 Clearinghouse*, Just Sec. (Dec. 1, 2023), <https://www.justsecurity.org/77022/january-6-clearinghouse/>.

<sup>169</sup> 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/>.

<sup>170</sup> 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>.

group that used the platform to promote “stakeouts” of ballot drop boxes.<sup>171</sup> The voter intimidation tactic was also discussed on Twitter, Telegram, Gab, and Craigslist.<sup>172</sup>

- 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.<sup>173</sup> 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.<sup>174</sup> 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.<sup>175</sup>
- 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.<sup>176</sup> For example, Facebook ads targeting Hispanic populations inaccurately described prominent

---

<sup>171</sup> 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>.

<sup>172</sup> 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-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>.

<sup>173</sup> 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>.

<sup>174</sup> 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>.

<sup>175</sup> *Id.*

<sup>176</sup> 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>.



American politicians as “communist” and compared them to socialist presidents in South America.<sup>177</sup>

- 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.<sup>178</sup>
- 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.<sup>179</sup>
- 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.<sup>180</sup>
- Meta developed an AI chatbot, and within a few days of studying online chatter, it began spreading election denialism and antisemitic conspiracy theories.<sup>181</sup>

### **Government benefits and services**

- Automated decision-making systems have erroneously disqualified individuals from food assistance benefits using a vague “criminal justice disqualification” criterion.<sup>182</sup> An algorithmic tool used by the Michigan Unemployment Insurance Agency to identify fraud in applications for unemployment benefits similarly incorrectly disqualified applicants.<sup>183</sup>
- 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

---

<sup>177</sup> 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>.

<sup>178</sup> 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>.

<sup>179</sup> 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/>.

<sup>180</sup> 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/>.

<sup>181</sup> 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>.

<sup>182</sup> Rashida Richardson et al., *Litigating Algorithms 2019 Report: New Challenges to Government Use of Algorithmic Decision Systems*, AI Now Inst., at 19–20 (Sept. 2019), <https://ainowinstitute.org/publication/litigating-algorithms-2019-u-s-report-2>.

<sup>183</sup> *Id.* at 20.



incorrect denials of benefits, particularly in communities of color.<sup>184</sup> 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 tax filings.<sup>185</sup> A year later, however, the IRS still did not have an alternative available.<sup>186</sup>

- 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.<sup>187</sup> Many Americans rely on these websites in large part due 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.<sup>188</sup>
- 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.<sup>189</sup> 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.<sup>190</sup> Among subgroups of

---

<sup>184</sup> 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>; see also *infra* § VI.C.1.

<sup>185</sup> See *infra* § VI.C.1.

<sup>186</sup> 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/>; 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/>.

<sup>187</sup> 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>.

<sup>188</sup> 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.”).

<sup>189</sup> 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](https://dho.stanford.edu/wp-content/uploads/IRS_Disparities.pdf).

<sup>190</sup> See *id.* at 4–5, 10.

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.<sup>191</sup>

## **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.<sup>192</sup> For example, one tool disproportionately predicted crime in neighborhoods that had higher populations of Black, Latino, and low-income residents, often predicting little to no crime in wealthier, whiter neighborhoods.<sup>193</sup> 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.<sup>194</sup>
- Facial recognition is widely used by law enforcement agencies despite well-established racial biases in the technology. 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.<sup>195</sup>
- Many jurisdictions use algorithms to predict recidivism risk when setting probation conditions, with little transparency as to the formulas and criteria considered.<sup>196</sup> The

---

<sup>191</sup> *Id.* at 28–29.

<sup>192</sup> 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/>.

<sup>193</sup> 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>.

<sup>194</sup> *Id.*

<sup>195</sup> 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](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/>.

<sup>196</sup> 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>.

American Bar Association passed a resolution urging that pretrial risk assessment tools should not be used unless they can be proven to be unbiased.<sup>197</sup>

- 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.<sup>198</sup>
- ShotSpotter, an audio gunshot detection technology, uses algorithms that are trained on data inputted by police officers.<sup>199</sup> ShotSpotter devices are overwhelmingly located in majority- or plurality-Black and Brown neighborhoods,<sup>200</sup> but there are significant doubts about their accuracy,<sup>201</sup> and the company has resisted transparency around its algorithms and systems.<sup>202</sup> ShotSpotter raises safety concerns about falsely triggering armed responses by anxious officers into predominantly Black neighborhoods and due process concerns about unreliable data being used as a basis for stops or arrests.<sup>203</sup>

---

<sup>197</sup> 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>.

<sup>198</sup> 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).

<sup>199</sup> 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>

<sup>200</sup> 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>.

<sup>201</sup> See Burke et al., *supra* note 199; 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).

<sup>202</sup> 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>.

<sup>203</sup> McBrien et al., *supra* note 200, at 21; see generally Harvey Gee, “Bang!”: *ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry’s Reach*, Univ. Mich. J. L. Reform 767 (2022), <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2561&context=mjlr>.

- Ring, operated by Amazon, routinely and voluntarily provides police access to video recordings from its cameras.<sup>204</sup> 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.<sup>205</sup> In exchange, departments agreed to promote Ring’s products.<sup>206</sup> Several cities maintain subsidy programs, encouraging residents to install Ring cameras at little or no cost.<sup>207</sup>
- 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.<sup>208</sup>
- 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 individuals.<sup>209</sup> Both companies have provided Immigration and Customs Enforcement (ICE) with access to sensitive personal information, including financial information, marriage records, and

---

<sup>204</sup> 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](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>.

<sup>205</sup> 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).

<sup>206</sup> 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>.

<sup>207</sup> 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/>.

<sup>208</sup> McBrien et al., *supra* note 200, at 19.

<sup>209</sup> 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/>.

addresses.<sup>210</sup> In a seven-month period, ICE ran over one million searches on their LexisNexis platforms.<sup>211</sup>

- 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.<sup>212</sup>
- 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.<sup>213</sup> The same broker has told Congress that data it is has sold to other brokers has subsequently been sold to law enforcement and the military.<sup>214</sup>
- 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.<sup>215</sup> Location data, search history, credit card transaction history, and

---

<sup>210</sup> See Cox, *supra* note 209; 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](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>.

<sup>211</sup> Biddle, *supra* note 210.

<sup>212</sup> 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>.

<sup>213</sup> 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>.

<sup>214</sup> 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>.

<sup>215</sup> 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>.



other information about everyday activities can be used to identify someone who has sought out reproductive or LGBTQ+ healthcare.<sup>216</sup>

- 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.<sup>217</sup>
- 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.<sup>218</sup>
- 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.<sup>219</sup>
- Absent any specific restrictions, many companies can sell or share data with law enforcement, ranging from motels sharing guest data with ICE for immigration enforcement<sup>220</sup> to genealogy and DNA companies sharing genetic data with the FBI,<sup>221</sup> to federal agencies simply buying cell phone location data in bulk.<sup>222</sup>

---

<sup>216</sup> 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>.

<sup>217</sup> 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/>.

<sup>218</sup> Caroline Haskins, *Amazon’s Home Security Company Is Turning Everyone Into Cops*, Vice: Motherboard (Feb. 7, 2019), <https://www.vice.com/en/article/qvyyzd/amazons-home-security-company-is-turning-everyone-into-cops>.

<sup>219</sup> 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>.

<sup>220</sup> 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/>.

<sup>221</sup> 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>.

<sup>222</sup> 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>.



- Geofence warrants<sup>223</sup> are increasingly being employed to exploit the large collections of users' location data amassed by tech companies like Google.<sup>224</sup> By its own numbers, Google received upwards of 10,000 geofence warrants in 2020, a more than 10 times increase since 2018.<sup>225</sup> 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.<sup>226</sup>
- In recent years, law enforcement has increasingly served so-called keyword search warrants on search engine providers, broadly demanding data on anyone who searched for a particular set of terms.<sup>227</sup> In addition to raising Fourth and First Amendment concerns,<sup>228</sup> dragnet warrants may also expose those seeking reproductive healthcare information to prosecution.<sup>229</sup>

---

<sup>223</sup> 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>.

<sup>224</sup> 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-chatrre-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-drag-nets-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>.

<sup>225</sup> 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](https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf) (see also the .csv data linked on page 2).

<sup>226</sup> 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/>.

<sup>227</sup> 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>.

<sup>228</sup> See *id.*

<sup>229</sup> 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>.

- ICE uses administrative subpoenas to obtain private records from tech and telecom companies.<sup>230</sup> 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.<sup>231</sup> ICE has a notable history of dragnet surveillance,<sup>232</sup> and its efforts threaten to sweep more people into an immigration enforcement system that is inextricably tied to racism and racial disparities.<sup>233</sup>
- 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.

---

<sup>230</sup> Dhruv Mehrotra, *ICE Is Grabbing Data From Schools and Abortion Clinics*, WIRED (Apr. 3, 2023), <https://www.wired.com/story/ice-1509-custom-summons/>.

<sup>231</sup> *Id.*

<sup>232</sup> See generally Wang et al., *supra* note 210.

<sup>233</sup> 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).