

**Before the  
Federal Trade Commission  
Washington, D.C.**

In the Matter of

Trade Regulation Rule on Commercial  
Surveillance and Data Security

**Commercial Surveillance ANPR,  
R111004**

**Lawyers' Committee for Civil Rights Under Law  
Comments in Response to the  
Advanced Notice of Proposed Rulemaking**

November 21, 2022

David Brody  
Katy Youker  
Sanaa Ansari  
Marc Epstein  
LAWYERS' COMMITTEE FOR CIVIL  
RIGHTS UNDER LAW  
1500 K Street, NW  
Suite 900  
Washington, DC 20005  
[www.lawyerscommittee.org](http://www.lawyerscommittee.org)

## Table of Contents

<b>I. Executive Summary</b> .....	<b>1</b>
<b>II. Segregation and redlining produced inequities that persist today and affect the data flowing in and out of commercial surveillance.</b> .....	<b>4</b>
A. Segregation denied Black Americans access to commerce and imposed upon them indignities and inequities.....	5
B. Redlining segregated and restricted opportunities for Black Americans to build wealth, find employment, receive education, and live in clean and healthy environments. ....	7
1. Educational consequences of segregation and redlining .....	8
2. Economic consequences of segregation and redlining .....	11
3. Health and environmental consequences of segregation and redlining .....	13
C. The history of surveillance is inextricably intertwined with white supremacy....	16
D. Lack of diversity in tech, historically and today, affects system design. ....	19
<b>III. Commercial surveillance harms are prevalent, including discriminatory uses of personal data and related civil rights issues</b> .....	<b>21</b>
A. Housing .....	24
B. Employment .....	28
C. Credit and finance .....	29
D. Insurance .....	31
E. Public health and healthcare .....	33
F. Education .....	37
G. Public accommodations .....	41
H. Online hate, harassment, and threats .....	44
I. Voter intimidation and election disinformation .....	48
J. Government benefits and services .....	52
K. Policing and law enforcement access to commercial surveillance .....	52
<b>IV. Discrimination is an unfair and deceptive trade practice</b> .....	<b>55</b>
A. Discrimination is an unfair trade practice. ....	57
1. Discrimination causes substantial injury to consumers. ....	57
2. Consumers cannot reasonably avoid the harms of discrimination; the act of avoidance is itself harmful.....	58
3. Discrimination does not have countervailing benefits. ....	60
B. Discrimination, if undisclosed, is a deceptive trade practice .....	65
C. The FTC Act applies to both intentional discrimination and disparate impact. .	66

D.	The FTC should recognize a diverse array of protected characteristics.....	68
<b>V.</b>	<b>The FTC has authority and responsibility to address discrimination and commercial surveillance practices.....</b>	<b>70</b>
A.	There are gaps in federal civil rights laws that the FTC can address.....	70
B.	The FTC can address gaps with its authority to regulate unfair and deceptive practices. It has done this before.....	74
C.	The FTC should consider how similar provisions of the Interstate Commerce Act were used to advance desegregation.....	79
<b>VI.</b>	<b>Effective rules must prohibit discriminatory commercial surveillance practices.....</b>	<b>82</b>
A.	Targeted advertising is an unfair trade practice.....	82
1.	Targeted advertising defined.....	83
2.	Targeted advertising causes substantial injury to consumers through segregation-based discrimination.....	86
3.	Consumers cannot reasonably avoid targeted advertising.....	88
4.	The benefits to consumers or competition do not outweigh the harms that targeted ads inflict.....	90
B.	Unchecked use of automated decision-making systems is likely to result in discrimination and is an unfair trade practice.....	92
1.	Automated decision-making systems place consumers at risk of substantial injury.....	93
2.	Consumers cannot reasonably avoid harms from discriminatory automated decision-making systems.....	94
3.	No countervailing benefits to consumers or competition outweigh the harms inflicted by discriminatory automated decision-making systems.....	95
4.	The Commission should implement the <i>AI Bill of Rights</i> and require pre- and post-deployment impact assessments.....	96
C.	Biometric technologies pose unique risks of harmful discrimination. Facial recognition is an unfair trade practice.....	98
1.	Facial recognition technology discriminates on the basis of race and gender; its use generally is an unfair trade practice.....	102
2.	Behavior recognition technologies lack a reliable scientific foundation, carry significant risk of bias and disparate impact, and should be restricted.....	109
<b>VII.</b>	<b>The FTC should establish robust privacy protections.....</b>	<b>112</b>
A.	Data collection, use, and sharing.....	113
1.	Data minimization.....	113
2.	Privacy by design and duty of loyalty.....	117
3.	Transparency.....	118

B.	Consumer rights.....	120
1.	Consumer’s right to access, correct, delete, and port personal data .....	120
2.	It is unfair to condition service upon a waiver of rights.....	122
3.	Consent can serve a limited role in discrete circumstances.....	124
C.	Data security .....	126
<b>VIII.</b>	<b>The FTC should set distinct rules to protect workers from unfair surveillance practices. ....</b>	<b>127</b>
A.	Already-pervasive commercial surveillance of workers has grown more prevalent during the COVID-19 pandemic and rise of the gig economy.....	128
1.	Workplace data-driven technologies in practice.....	129
2.	Workplace surveillance has become more ubiquitous since the COVID-19 pandemic. ....	131
3.	The gig economy has created new opportunities for worker surveillance...	134
B.	Worker surveillance that undermines workers’ rights is an unfair or deceptive trade practice.....	135
1.	Workers face unique and substantial harms from commercial surveillance.	135
2.	Workers have no practical means to avoid harms from workplace surveillance.	139
3.	Putative benefits of worker surveillance used to violate workers’ rights do not outweigh the harms.....	140
C.	Guidance for rules to limit the harms of worker surveillance. ....	141
<b>IX.</b>	<b>The First Amendment does not block FTC action to protect civil rights and privacy.....</b>	<b>144</b>
A.	Algorithmic systems, including targeted advertising, involve unprotected conduct and otherwise merely incidentally affect speech.....	145
B.	If speech is implicated, it is commercial speech subject to lesser protection under the First Amendment. ....	147
C.	Even if non-commercial speech is implicated, preventing fraud, discrimination, and voter intimidation are compelling government interests. ....	148
<b>X.</b>	<b>Conclusion .....</b>	<b>149</b>
	<b>Appendix A: ANPR Questions Addressed in Lawyers’ Committee’s Comments</b>	<b>151</b>

## I. Executive Summary<sup>1</sup>

Privacy rights are civil rights. The “inviolability of privacy” is “indispensable to preservation of freedom of association.”<sup>2</sup> We care about data privacy because it ensures that who we are cannot be used against us unfairly. By protecting privacy, we come closer to building an equitable internet, one that can empower communities of color and open doors for enfranchised populations. An equitable internet promises the freedom to define oneself, organize, advocate, learn, play, pray, and build.

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. Commercial surveillance poses a threat to equality of opportunity and autonomy. The Federal Trade Commission (the “FTC” or “Commission”) has an affirmative role to play in building a digitized society that rejects a new form of “Jim Code”: “the employment of new technologies that reflect and reproduce existing inequities but that are promoted and perceived as more objective or progressive than the discriminatory systems of a previous era.”<sup>3</sup>

The Lawyers’ Committee for Civil Rights Under Law (the “Lawyers’ Committee”) uses legal advocacy to achieve racial justice, fighting inside and outside the courts to ensure that Black people and other people of color have voice, opportunity, and power to make the promises of our democracy real. The Lawyers’ Committee’s Digital Justice Initiative works at the intersection of racial justice, technology, and privacy to address predatory commercial data practices, discriminatory algorithms, invasions of privacy, disinformation, and online harms that disproportionately affect Black people and other people of color, including people with intersectional identities, like immigrants, women of color, and LGBTQ people of color.

In these comments, the Lawyers’ Committee responds to the questions in the Advanced Notice of Proposed Rulemaking (the “ANPR”) and discusses (1) the history and ongoing legacies of segregation and redlining, and how they relate to commercial surveillance today; (2) examples of harms caused by commercial surveillance practices, including discrimination in housing, employment, credit, insurance, healthcare, education, and

---

<sup>1</sup> The Lawyers’ Committee is grateful for assistance in the preparation of these comments by the students and faculty of the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley School of Law, including Cecily Kruger, Savannah Grossarth Nuttall, and Christian Howard-Sukhil.

<sup>2</sup> *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958).

<sup>3</sup> See Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* 5–6 (2019).

public accommodations, as well as voter suppression, disinformation, amplification of white supremacy, and exacerbation of the over-policing of communities of color; (3) why discrimination is an unfair and deceptive trade practice under the FTC Act; (4) the FTC's role in the advancement of civil rights; (5) other commercial surveillance practices that are unfair and deceptive, including targeted advertising, unbounded use of automated decision-making systems, and biometric technologies such as facial recognition; (6) consumer privacy rules the FTC should enact to prevent unfairness and deception; (7) the need for distinct protections against commercial surveillance of workers; and (8) the FTC's ability to address these issues consistent with the First Amendment. At the end of these comments is an Appendix listing each ANPR question we address and in which sections they are addressed, for ease of reference.

Systematic discrimination in this context involves the collection and use of the personal data of individuals to discern their race, religion, sex, and other traits for the purpose of segmenting and subjugating populations in disparate ways. And it involves data sharing among gatekeepers, private or public, who insulate class-based hierarchies against meritocratic performance and equal opportunity. In contrast, interventions that block discriminatory data uses can directly impede the cogs and gears of white supremacy. This is part of the reason why privacy, “the right to be let alone,” is often considered “the most comprehensive of rights.”<sup>4</sup>

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 white supremacist 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. The consequences of residential and educational segregation are still with us. Disparities in employment and credit opportunities, and resulting disparities in intergenerational wealth generation, are still endemic. Access to healthcare and clean environments is unequal. Disinformation and online hate disproportionately target communities of color. The ongoing consequences of segregation are legion: “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>5</sup> The effects of discrimination are literally in the blood of Black America, manifesting as

---

<sup>4</sup> *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

<sup>5</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).

disproportionate incidences of inflammatory diseases.<sup>6</sup> 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>7</sup>

In a society scaffolded on top of the consequences of institutionalized oppression, automated decision-making systems often reproduce discrimination. At the root of algorithmic bias is the reckless 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>8</sup> These mistaken shortcuts fail to account for the fact that while a person may be in part a product of their circumstances, that does not mean they necessarily *are* or *should be* limited by those circumstances. That is the essence of unfairness and is fundamentally at odds with the promise of the American Experiment, “the land that never has been yet—/ And yet must be—the land where every man is free.”<sup>9</sup>

The FTC should use its longstanding authority to regulate unfair and deceptive trade practices to combat segregation, prohibit discriminatory data uses, and protect privacy. The internet is not coded on a blank slate. The future of equal opportunity depends on whether we allow the data-driven economy of the 21st century to replicate the inequities of prior centuries. Given the prevalent and ongoing harms, we urge the Commission to promulgate such rules without delay.

---

<sup>6</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/researchers/research-digests/skin-deep-resilience/> (last visited Nov. 1, 2022).

<sup>7</sup> *Jones v. Alfred H. Mayer Co.*, 392 U.S. 409, 443 (1968) (cleaned up).

<sup>8</sup> See generally 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).

<sup>9</sup> Langston Hughes, *Let America Be America Again* (1936) (emphasis in original).

## II. Segregation and redlining produced inequities that persist today and affect the data flowing in and out of commercial surveillance.

The Commission asks, in questions 24, 25, and 39, how to weigh, and on what time horizon, the costs and benefits of commercial surveillance practices and regulations.<sup>10</sup> It asks in questions 29 and 50 about the benefits or costs of refraining from promulgating new rules on commercial surveillance and data security.<sup>11</sup> And it asks in question 68 whether and how to consider harms to protected classes and underserved groups.<sup>12</sup> As the Commission weighs these and related questions, it should consider the history of segregation and redlining, their lasting effects that persist to this day, and the intersection of systemic racism with current commercial surveillance and automated decision-making practices.

Commercial surveillance practices today have their origins in separate-but-equal segregation, which denied equal opportunity to millions. The analog version of a discriminatory algorithm was redlining, which deprived communities of color of intergenerational wealth and health. This one algorithmic system—using racial geography as part of a formula for determining government subsidies for homeownership and built on top of segregated housing—has caused a *century* of devastating downstream effects with no end in sight.

Across every sector of the economy and every facet of American life, our present-day status quo is inextricably intertwined with the unresolved consequences of slavery, segregation, and systemic racism. Data drawn from this form of American exceptionalism necessarily echo and reflect the painful policy choices of yesteryear—and choices we continue to make today. New technologies are not operating on neutral starting positions. Commercial surveillance technologies and practices that turn a blind eye to *why* the data say what they say inevitably and irresponsibly replicate and amplify systematic discrimination.

As will be discussed below, discrimination is harmful and costly to the economy and society as a whole, beyond just the aggregation of its effects on individuals. Commercial surveillance technologies, if not implemented extremely carefully, are likely to

---

<sup>10</sup> FTC Trade Regulation Rule on Commercial Surveillance and Data Security (“ANPR”), 16 C.F.R. pt. 464, 87 Fed. Reg. 51273, 51282–83 (2022).

See Appendix A for a list of each question addressed in these comments and in which sections they are addressed.

<sup>11</sup> *Id.* at 51283.

<sup>12</sup> *Id.* at 51284.

perpetuate, replicate, and amplify segregation. A failure to act now risks a continuation of the harms of systemic racism through the data-driven economy.

**A. Segregation denied Black Americans access to commerce and imposed upon them indignities and inequities.**

At the time of the Civil War, 88% of the U.S. Black population (3.9 million people) lived in the Confederacy and were subjected to the horrific institution of slavery.<sup>13</sup> According to W.E.B. Dubois, after slavery was abolished the “slave went free; stood a brief moment in the sun; then moved back again toward slavery.”<sup>14</sup> In the post-Reconstruction United States, states ushered in the Jim Crow era by systematically relegating Black people to second-class citizenship. They did so by enacting laws, ordinances, and customs that separated white and Black people in every conceivable area of life.<sup>15</sup> This code of segregation “lent the sanction of law to a racial ostracism that extended to churches and schools, to housing and jobs, to eating and drinking,” and “that ostracism extended to virtually all forms of public transportation, to sports and recreations, to hospitals, orphanages, prisons, and asylums, and ultimately to funeral homes, morgues, and cemeteries.”<sup>16</sup> Racial segregation was not limited to the postbellum South. To the contrary, some northern states maintained separate schools for Black children and had laws against interracial marriage.<sup>17</sup>

Following the Supreme Court’s holding in *The Civil Rights Cases* that the 13th and 14th Amendments did not authorize Congress to prohibit discrimination in places of public accommodation,<sup>18</sup> Southern states responded with a steady onslaught of legislation to ensure that Black people remained segregated in nearly every aspect of society.<sup>19</sup> “The supply of ideas for new ways to segregate seemed inexhaustible,” and “[n]umerous

---

<sup>13</sup> U.S. Census Bureau, *1860 Census: Population of the United States* vi–viii (1860), <https://www2.census.gov/library/publications/decennial/1860/population/1860a-02.pdf>.

<sup>14</sup> W.E.B. Dubois, *Black Reconstruction: An Essay Toward a History of the Part Which Black Folk Played in the Attempt to Reconstruct Democracy in America, 1860-1880* 26 (Routledge ed., 2017).

<sup>15</sup> C. Vann Woodward, *The Strange Career of Jim Crow* 7 (1955).

<sup>16</sup> *Id.*

<sup>17</sup> See John Hope Franklin, *History of Racial Segregation in the United States*, 304 *Annals Am. Academy Pol. & Soc. Sci.* 1, 1–9 (1956).

<sup>18</sup> See *The Civil Rights Cases*, 109 U.S. 3, 25 (1883). *But see Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 250–62 (1964) (holding that Congress has authority under the Commerce Clause to enact anti-discrimination legislation).

<sup>19</sup> See Franklin, *supra* note 17, at 6–9.

devices were employed to perpetuate segregation in housing, education, and places of public accommodation,” including “[s]eparate Bibles for oath taking in courts of law, separate doors . . . separate elevators and stairways, [and] separate drinking fountains.”<sup>20</sup> And, where laws left gaps, informal codes filled them. So eager were states to divide people based on race that “separate toilets existed even where the law did not require them.”<sup>21</sup>

Private businesses in the Jim Crow era routinely refused to provide publicly available goods and services to people of color. So ubiquitous was this private discrimination that Black people traveling within the United States turned to guides like *The Green Book* to learn where they could safely access hotels, restaurants, gas stations, and other types of businesses.<sup>22</sup> The introduction to the 1948 edition offered a poignant observation about the state of private discrimination in the era:

There will be a day sometime in the near future when this guide will not have to be published. That is when we as a race have equal opportunities and privileges in the United States. It will be a great day for us to suspend this publication for then when we can come and go as we please, and without embarrassment. But until that time comes we shall continue to publish this information for your convenience each year.<sup>23</sup>

After numerous legal challenges and non-violent resistance to racial segregation in places of public accommodation, the federal government enacted the Civil Rights Act of 1964. Title II of that act prohibited discrimination by entitling everyone in this country to “the full and equal enjoyment of the goods, services, facilities, privileges, advantages, and accommodations of any place of public accommodation . . . without discrimination or segregation on the ground of race, color, religion, or national origin.”<sup>24</sup> A watershed enactment, Title II aimed to eliminate the loss of “personal dignity that surely accompanies denials of equal access to public establishments.”<sup>25</sup> The Senate Commerce Committee’s report stressed that “[d]iscrimination is not simply dollars and cents, hamburgers and

---

<sup>20</sup> *Id.* at 8.

<sup>21</sup> *Id.*

<sup>22</sup> The New York Public Library has digitized many years’ worth of *The Green Book*. They are available at <https://digitalcollections.nypl.org/collections/the-green-book>.

<sup>23</sup> *The Green Book* (Victor H. Green ed., 1948), [https://digitalcollections.nypl.org/items/6fa574f0-893f-0132-1035-58d385a7bbd0#](https://digitalcollections.nypl.org/items/6fa574f0-893f-0132-1035-58d385a7bbd0#/).

<sup>24</sup> 42 U.S.C. § 2000a(a).

<sup>25</sup> S. Rep. No. 88-872 (1964), *reprinted in* 1964 U.S.C.C.A.N. 2355, 2370.

movies; it is the humiliation, frustration, and embarrassment that a person must surely feel when he is told that he is unacceptable as a member of the public because of his race or color.”<sup>26</sup>

**B. Redlining segregated and restricted opportunities for Black Americans to build wealth, find employment, receive education, and live in clean and healthy environments.**

For decades, redlining and housing discrimination have segregated entire communities and cities. This produced and still perpetuates racially segregated neighborhoods where many Americans reside, isolated from high-performing public schools, good jobs, safe streets, reliable public services, and a clean and healthy environment. Such isolation has intergenerational effects that continue to limit the opportunities available to emerging generations.<sup>27</sup> And those effects manifest in data about these communities and the people who live in them—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.

Beginning before World War II and continuing thereafter, government agencies including the Home Owners Loan Corporation, Fannie Mae, and the Federal Housing Administration (FHA) fueled the creation of suburban America through low-cost mortgage loans to developers and homebuyers in a manner that excluded people of color. The Home Owners’ Loan Corporation specifically mapped out America’s racial geography, drawing red lines around Black neighborhoods and marking them as off limits for government-insured mortgages. Both the FHA and Fannie Mae refused to support the origination of mortgages to Black people or insure any project where developers had not taken adequate steps to ensure that no homes would be sold to Black buyers.<sup>28</sup> As developers built homes using federal dollars conditioned on selling to white families, they solicited white buyers;<sup>29</sup> targeted advertising to prospective white buyers played a key role in creating and perpetuating the segregated housing system. When Black Americans were able to acquire homes they were often charged more than they would have paid under an FHA mortgage and had fewer protections, adding up to billions in lost wealth generation

---

<sup>26</sup> *Id.*

<sup>27</sup> See Patrick Sharkey, *Stuck in Place: Urban Neighborhoods and the End of Progress Toward Racial Equality* 9–10, 91–116 (Univ. of Chicago Press 2013).

<sup>28</sup> See Richard Rothstein, *The Color of Law: A Forgotten History of How Our Government Segregated America* 18–24 (2017).

<sup>29</sup> See, e.g., Douglas S. Massey & Nancy A. Denton, *American Apartheid: Segregation and the Making of the Underclass* 20 (1993).

through predatory interest and inability to build home equity.<sup>30</sup> Redlining was a primitive algorithm that caused systemic and systematic discrimination both directly and through the market incentives and business practices that flowed downstream from it.

Residential segregation and its effects continue today.<sup>31</sup> The consequences of redlining for communities of color are broad, deep, and persistent. “Many measures of resource distribution and public well-being now track the same geographic pattern: 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>32</sup> Due to the legacy of redlining and ongoing disinvestment from communities of color, the effects of living in segregated neighborhoods with high levels of concentrated poverty are overwhelmingly adverse across several dimensions: restricting access to education, employment, and public services, and negatively impacting health. The effects on children are particularly acute and resonate across generations. Conversely, removing barriers to residential integration delivers broadly felt social benefits.

## 1. Educational consequences of segregation and redlining

Equal housing opportunity is closely linked with educational diversity and achievement. “Public schools typically reflect their neighborhood demographics because most students are assigned to schools based on their residence.”<sup>33</sup> The Supreme Court has

---

<sup>30</sup> See, e.g., Samuel Dubois Cook Ctr. on Soc. Equity, *The Plunder of Black Wealth in Chicago: New Findings on the Lasting Toll of Predatory Housing Contracts* iii (May 2019) (“The average black buyer paid several points more in interest on their contract loan than the average white buyer paid on a conventional or FHA backed mortgage.”), <https://socialequity.duke.edu/wp-content/uploads/2019/10/Plunder-of-Black-Wealth-in-Chicago.pdf>.

<sup>31</sup> See William H. Frey, *Growth, diversity, segregation, and aging in America’s largest metropolitan areas: A 2020 census portrait*, Brookings (May 13, 2022), <https://www.brookings.edu/research/growth-diversity-segregation-and-aging-in-americas-largest-metropolitan-areas-a-2020-census-portrait/>.

<sup>32</sup> *Leaders of a Beautiful Struggle*, 2 F.4th at 349 (Gregory, C.J., concurring); see also Marceline White, *Baltimore: The Black Butterfly*, National Community Reinvestment Coalition (Oct. 8, 2020), <https://ncrc.org/the-black-butterfly/>; Urban Inst., *The Black Butterfly: Racial Segregation and Investment Patterns in Baltimore* (Feb. 5, 2019), <https://apps.urban.org/features/baltimore-investment-flows>.

<sup>33</sup> Roslyn Arlin Mickelson, *Exploring the School-Housing Nexus: A Synthesis of Social Science Evidence*, in *Finding Common Ground: Coordinating Housing and Education*

also recognized that choices regarding the location of schools “have been used as a potent weapon for creating or maintaining a state-segregated school system.”<sup>34</sup> “School segregation is tethered to residential segregation because of the prevalence of neighborhood schools in the public education system. This linkage is especially strong at the lower grades.”<sup>35</sup>

School segregation significantly limits educational opportunities and outcomes for students of color.<sup>36</sup> Segregation in education impairs students’ ability to learn, as integration can be a powerful force for improved learning.<sup>37</sup> High levels of segregation often result in resource disparities that lead to detrimental outcomes, including larger class sizes, lower funding, fewer resources, more inexperienced teachers, insufficient facilities, lower per-pupil spending, and reduced access to services like counseling.<sup>38</sup> These

---

*Policy to Promote Integration* 5 & n.1 (Philip Tegeler, ed., Poverty & Race Research Action Council & National Coalition on School Diversity, 2011), <http://www.prrac.org/pdf/HousingEducationReport-October2011.pdf>; see also Simon Burgess & Adam Briggs, *School Assignment, school choice, and social mobility*, 29 Econ. Educ. Rev. 639 (2010); Deenesh Sohoni & Salvatore Saporito, *Mapping School Segregation: Using GIS to Explore Racial Segregation Between Schools and Their Corresponding Attendance Areas*, 115 Am. J. Educ. 569 (2009).

<sup>34</sup> *Swann v. Charlotte-Mecklenburg Bd. of Educ.*, 402 U.S. 1, 21 (1971).

<sup>35</sup> Paul M. Ong & Jordan Rickles, *The Continued Nexus Between School and Residential Segregation*, 6 Afr.-Am. L. & Pol’y Rep. 178, 179 (2004).

<sup>36</sup> See Gary Orfield et al., *E Pluribus... Separation: Deepening Double Segregation for More Students*, The Civil Rights Project, at 6–10 (Sept. 2012, rev. Oct. 18, 2012), <https://civilrightsproject.ucla.edu/research/k-12-education/integration-and-diversity/mlk-national/e-pluribus...separation-deepening-double-segregation-for-more-students/orfield-epluribus-revised-omplete-2012.pdf>; Dennis J. Condrón, *Social Class, School and Non-School Environments, and Black/White Inequalities in Children’s Learning*, 74 Am. Soc. Rev. 683, 699 (2009).

<sup>37</sup> See Douglas N. Harris, *Lost Learning, Forgotten Promises: A National Analysis of School Racial Segregation, Student Achievement, and “Controlled Choice” Plans*, Ctr. for Am. Progress (Nov. 24, 2006), <http://cdn.americanprogress.org/wp-content/uploads/issues/2006/11/pdf/lostlearning.pdf>.

<sup>38</sup> See Marguerite L. Spencer et al., *The Benefits of Racial and Economic Integration in Our Education System: Why This Matters for Our Democracy*, Kirwan Inst. for the Study of Race & Ethnicity 9 (Feb. 2009), <https://kirwaninstitute.osu.edu/research/benefits-racial-and-economic-integration-our-education-system>; Brief for 553 Social Scientists as *Amici Curiae* Supporting Respondents, *Parents Involved in Cmty. Schs. v. Seattle Sch. Dis. No. 1*, 551 U.S. 701 (2007) (Nos. 05-908, 05-915); Roslyn Arlin Mickelson, *When are Racial Disparities in Education the Result of Racial Discrimination? A Social Science Perspective*, 105 Tchrs. Coll. Rec. 1052, 1061–62 (2003); see also U.S. Dep’t of Justice & U.S.

disparities can produce data that can be collected and used without accounting for its context and enable replication of patterns of discrimination; for example, gaps in test scores and reading ability increase as racial segregation increases.<sup>39</sup> Racially segregated schools account for the majority of the nation's high schools with significantly elevated dropout rates, while integrated school environments are associated with lower dropout rates.<sup>40</sup> This too produces data about educational attainment and future employment prospects that will be collected and used by large data models.

Conversely, compelling evidence demonstrates that attending integrated schools is associated with a host of positive educational and life outcomes.<sup>41</sup> Low-income, students of color perform better academically in diverse school settings, with improvements resulting from significant peer effects and the reduction of resource disparities. In addition, research has found that students of all racial backgrounds tend to perform better academically in racially integrated schools, compared to those who attend schools that are

---

Dep't of Educ., *Guidance on the Voluntary Use of Race to Achieve Diversity and Avoid Racial Isolation in Elementary and Secondary Schools* 1–2 (Nov. 2011), <http://www2.ed.gov/about/offices/list/ocr/docs/guidance-ese-201111.pdf>; Orfield et al, *supra* note 36.

<sup>39</sup> See Mark Berends & Roberto Peñaloza, *Increasing Racial Isolation and Test Score Gaps in Mathematics: A 30-year Perspective*, 112 *Tchrs. Coll. Rec.* 978 (2010); Shelly Brown-Jeffy, *The Race Gap in High School Reading Achievement: Why School Racial Composition Still Matters*, 13 *Race, Gender & Class* 268 (2006).

<sup>40</sup> See Robert Balfanz & Nettie Legters, *Locating the Dropout Crisis: Which High Schools Produce the Nation's Dropouts? Where Are They Located? Who Attends Them?* (2004), <http://files.eric.ed.gov/fulltext/ED484525.pdf>; Jonathan Guryan, *Desegregation and Black Dropout Rates*, 94 *Am. Econ. Rev.* 919, 931–32 (2004).

<sup>41</sup> See Rucker C. Johnson, *Long-run Impacts of School Desegregation & School Quality on Adult Attainments* 2–3 (Nat'l Bur. of Econ. Res., Working Paper No. 16664, Jan. 2011, rev. Sept. 2015), <http://www.nber.org/papers/w16664>.

racially and socioeconomically isolated.<sup>42</sup> Racially and socioeconomically integrated schools also have higher rates of graduation than high-poverty, segregated schools.<sup>43</sup>

The degree of integration in educational settings also affects the neighborhoods students are likely to seek to live in as adults. “The experience of attending segregated schools has intergenerational consequences for adults’ choices of same or different race neighbors. Students who attended more racially isolated elementary, middle, and high schools are more likely as adults to prefer same race neighbors compared to adults who have attended integrated schools.”<sup>44</sup>

## 2. Economic consequences of segregation and redlining

Historic redlining and segregation deprived Black Americans of employment opportunities and economic advancement; it stymied intergenerational wealth generation beyond just home equity. As Senator Walter Mondale, a sponsor of the Fair Housing Act, said, “Unless [Black Americans] are going to be able to move in the suburban communities through the elimination of housing discrimination and the provision of low- and moderate-cost housing, they are going to be deprived of many jobs because they will be unable to live in the central city and work in the suburbs.”<sup>45</sup>

Today, segregation continues to impede access to employment and other resources, such that poverty remains entrenched and mobility out of reach to many people

---

<sup>42</sup> See Susan Eaton, *How the Racial and Socioeconomic Composition of Schools and Classrooms Contributes to Literacy, Behavioral Climate, Instructional Organization and High School Graduation Rates* 1 & n. 1 (Nat’l Coal. on Sch. Diversity Res. Brief No. 2, Oct. 2010, rev. Mar. 2011), <http://school-diversity.org/pdf/DiversityResearchBriefNo2.pdf>; Gary Orfield & Chungmei Lee, *Why Segregation Matters: Poverty and Educational Equality*, The Civil Rights Project, at 15, (Jan. 2005), <http://civilrightsproject.ucla.edu/research/k-12-education/integration-and-diversity/why-segregation-matters-poverty-and-educational-inequality/orfield-why-segregation-matters-2005.pdf>.

<sup>43</sup> See Christopher B. Swanson, *Who Graduates? Who Doesn’t?: A Statistical Portrait of Public High School Graduation, Class of 2001*, Urban Inst. Educ. Pol’y Ctr. 35 (2004), <https://www.urban.org/research/publication/who-graduates-who-doesnt>.

<sup>44</sup> Mickelson, *supra* note 33, at 6–7; see also Roslyn Arlin Mickelson & Mokubung Nkomo, *Integrated Schooling, Life Course Outcomes, and Social Cohesion in Multiethnic Democratic Societies*, 36 Rev. of Rsch. in Educ. 197, 218–19 (Mar. 2012), [http://www.school-diversity.org/pdf/Mickelson\\_Nkomo\\_%20RRE\\_2012.pdf](http://www.school-diversity.org/pdf/Mickelson_Nkomo_%20RRE_2012.pdf); Jomills Henry Braddock II & Amaryllis Del Carmen Gonzalez, *Social Isolation and Social Cohesion: The Effects of K-12 Neighborhood and School Segregation on Intergroup Orientations*, 112 Tchrs. Coll. Rec. 1631 (2010).

<sup>45</sup> 114 Cong. Rec. 2276 (1968) (statement of Sen. Mondale).

of color. “Segregation . . . isolates disadvantaged groups from access to public and private resources, from sources of human and cultural capital, and from the social networks that govern access to jobs, business connections, and political influence.”<sup>46</sup>

Online social networks are derived in large part from real world social networks. Absent careful consideration of the data being used to recommend “who you may know” or other social capital opportunities, these systems can easily reinforce segregation.

Employment discrimination is more prevalent and harder to combat in poor communities as well. Between 1998–2017, 19% of employment discrimination cases were litigated *pro se* because many workers lack the resources necessary to hire an attorney.<sup>47</sup> Even when workers are able to secure “expensive and often elusive legal representation . . . [e]mpirical studies of employment law claims show that plaintiffs have limited success at every level of the process.”<sup>48</sup> Because it is so difficult to bring employment discrimination claims after the fact, particularly for low income workers of color, it is particularly important to structure commercial surveillance rules in a manner that *prevents* discrimination in the first place.

Integration of residential areas is crucial to expanding access to jobs. In metropolitan areas characterized by higher job sprawl, residential segregation is an independent factor that contributes to Black Americans’ physical isolation from jobs.<sup>49</sup> The geographic mismatch between job sites and segregated neighborhoods often results in racial and ethnic differences in income due to the relocation of high-paying, low-skilled jobs away from the cities and older suburbs.<sup>50</sup> Where Black Americans are most segregated from whites residentially, they are also likely to experience the greatest mismatch between their residences and available jobs.<sup>51</sup> Racial isolation constricts the social networks of

---

<sup>46</sup> Elizabeth Anderson, *The Imperative of Integration 2* (2010).

<sup>47</sup> Mitchell Levy, *Empirical Patterns of Pro Se Litigation in Federal District Courts*, 85 U. Chi. L. Rev. 1819, 1841 (2018).

<sup>48</sup> Ann C. Hodges, *The Limits of Multiple Rights and Remedies: A Call for Revisiting the Law of the Workplace*, 22 Hofstra Lab. & Emp. L.J. 601, 611 (2005); see also Phyllis Tropper Baumann et al., *Substance in the Shadow of Procedure: The Integration of Substantive and Procedural Law in Title VII Cases*, 33 B.C. L. Rev. 211, 289 (1992) (“[T]itle VII plaintiffs typically are economically insecure.”).

<sup>49</sup> Michael A. Stoll, *Job Sprawl and the Spatial Mismatch between Blacks and Jobs*, Brookings Inst. Metro. Pol’y Program, at 7 (Feb. 2005), <https://www.brookings.edu/research/job-sprawl-and-the-spatial-mismatch-between-blacks-and-jobs/>.

<sup>50</sup> See generally *id.*

<sup>51</sup> *Id.* at 8.

people of color, limiting employment opportunities.<sup>52</sup> Fewer employment opportunities means less social mobility and wealth generation, affecting huge swaths of societal and consumer spending data.

Residential segregation also leads to a lack of access to other communal, commercial, and economic opportunities that do not get built or developed in majority-minority areas. For example, communities of color are less likely to benefit from reliable municipal services,<sup>53</sup> or to enjoy access to grocery stores and fresh foods,<sup>54</sup> private-practice healthcare facilities,<sup>55</sup> and green spaces, such as parks and sports fields.<sup>56</sup>

As the Commission grapples with how to set privacy rules, it must contend with the fact that data about *practically every aspect of the economy* is affected by downstream effects of systemic racism.

### **3. Health and environmental consequences of segregation and red-lining**

Segregation causes tangible injuries to the health of Black and Brown Americans—both directly through health effects caused by discrimination and indirectly through toxic exposures from pollution dumped on communities of color. The consequences of these health effects will show up in health data and data about related products and services, potentially resulting in racially disparate impacts when such data is used at scale to make decisions.

---

<sup>52</sup> Douglas S. Massey & Nancy A. Denton, *American Apartheid* 109, 161–62, 166 (1993).

<sup>53</sup> See, e.g., *Comm. Concerning Cmty. Improvement v. City of Modesto*, 583 F.3d 690 (9th Cir. 2009); *Kennedy v. City of Zanesville*, 505 F. Supp. 2d 456 (S.D. Ohio 2007); *Lopez v. City of Dallas*, No. 3:03-cv-2223-M, 2004 WL 2026804 (N.D. Tex. Sept. 9, 2004).

<sup>54</sup> See, e.g., Michele Ver Ploeg et al., *Mapping Food Deserts in the United States*, U.S. Dep't of Agri. Econ. Res. Serv. (Dec. 1, 2011), <https://www.ers.usda.gov/amber-waves/2011/december/data-feature-mapping-food-deserts-in-the-us/>; Kimberly Morland et al., *Neighborhood Characteristics Associated with the Location of Food Stores and Food Service Places*, 22 *Am. J. Prev. Med.* 23 (2002).

<sup>55</sup> See, e.g., Jamila Taylor, *Racism, Inequality, and Health Care for African Americans*, The Century Foundation (Dec. 19, 2019), <https://tcf.org/content/report/racism-inequality-health-care-african-americans/>; David Barton Smith, *Health Care Divided: Race and Healing a Nation* 283 (1999).

<sup>56</sup> See Ming Wen et al., *Spatial Disparities in the Distribution of Parks and Green Spaces in the USA*, 45 *Annals Behav. Med.* 18 (2013); Dustin T. Duncan et al., *The Geography of Recreational Open Space: Influence of Neighborhood Racial Composition and Neighborhood Poverty*, 90 *J. Urb. Health* 618 (2012).

Black Americans who grow up in impoverished or segregated areas and go on to achieve upward socioeconomic mobility pay a physiological price for overcoming adversity. “Specifically, a growing consensus is emerging regarding a hidden cost to resilience, particularly as it relates to *physical health*.”<sup>57</sup> “In a sample of nearly 500 rural African American youth . . . outwardly resilient youth also reported higher levels of *allostatic load*, a biological marker of wear-and-tear on multiple bodily systems.”<sup>58</sup> These results have been repeatedly confirmed.<sup>59</sup> This can lead to negative health outcomes related to “cellular aging, diabetes risk, metabolic syndrome, and respiratory infection.”<sup>60</sup> In sum, there is a physical health cost to overcoming the poverty and discrimination resulting from segregation: a constant high level of stress hormones in the body that causes inflammation and related diseases.<sup>61</sup>

Segregation also correlates with environmental quality—people of color have often been forced to live in polluted areas and pollution-generating industries are more likely to be placed near communities of color. That in turn causes negative health effects which will, again, manifest in health and other data. Racially or ethnically isolated communities are much more likely to experience environmental hazards and associated adverse health impacts than are integrated communities, making race a stronger corollary to environmental vulnerability than income.<sup>62</sup> It was first identified in 1987, and repeatedly confirmed, “that race was consistently a more prominent factor in the location of commercial

---

<sup>57</sup> Ctr. for Fam. Rsch., *supra* note 6; see also Gene H. Brody et al., *Is resilience only skin deep? Rural African Americans’ socioeconomic status-related risk and competence in preadolescence and psychological adjustment and allostatic load at age 19*, 24 *Psych. Sci.* 1285, 1285–93 (2013), <https://journals.sagepub.com/doi/10.1177/0956797612471954> (emphasis in original); see also Gregory E. Miller et al., *Youth who achieve upward socioeconomic mobility display lower psychological distress but higher metabolic syndrome rates as adults: Prospective evidence from the National Study of Add Health and MIDUS*, 9 *J. of the Am. Heart Ass’n* e015698 (2020), <https://www.ahajournals.org/doi/10.1161/JAHA.119.015698>.

<sup>58</sup> Ctr. for Fam. Rsch., *supra* note 6 (emphasis in original).

<sup>59</sup> See *id.* (discussing research on this subject).

<sup>60</sup> *Id.*

<sup>61</sup> See Ctr. for Fam. Rsch., *John Henryism*, <https://cfr.uga.edu/for-researchers/research-digests/john-henryism/> (last visited Nov. 2, 2022); Sherman A. James, *John Henryism and the health of African-Americans*, 18 *Culture, Med., & Psychiatry* 163, 163–82 (1994), <https://doi.org/10.1007/BF01379448>.

<sup>62</sup> See, e.g., 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’tl. 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).

hazardous waste facilities than any other factor examined.”<sup>63</sup> Hazardous materials disposal sites, municipal waste facilities, power plants, and other sources of pollution are all disproportionately located in racially and ethnically identifiable communities of color,<sup>64</sup> in a way that neither housing preferences nor wealth gaps adequately explain.<sup>65</sup> Residents of segregated communities are significantly more likely to experience high-volume releases of toxic chemicals,<sup>66</sup> to breathe high concentrations of harmful air pollutants,<sup>67</sup> and to live in chronically substandard, lead-painted housing.<sup>68</sup>

---

<sup>63</sup> United Church of Christ, Comm’n for Racial Justice, *Toxic Wastes and Race in the United States: A National Report of the Racial and Socio-Economic Characteristics of Communities with Hazardous Waste Sites* 15 (1987), <https://uccfiles.com/pdf/Toxic-Wastes&Race.pdf>; see also U.S. Gen. Accounting Off., *Siting of Hazardous Waste Landfills and Their Correlation with Racial and Economic Status of Surrounding Communities* (1983), <http://archive.gao.gov/d48t13/121648.pdf>; see generally Robert D. Bullard et al., *Toxic Wastes and Race at Twenty: 1987-2007*, 38–47 (2007), <https://www.ucc.org/wp-content/uploads/2021/03/toxic-wastes-and-race-at-twenty-1987-2007.pdf>; U.S. Comm’n on Civil Rights, *Not in My Backyard: Executive Order 12,898 and Title VI as Tools for Achieving Environmental Justice* 16–19 (2003), <https://www.usccr.gov/files/pubs/en-just/ej0104.pdf>; Luke W. Cole & Sheila R. Foster, *From the Ground Up: Environmental Racism and the Rise of the Environmental Justice Movement* 167–83 (2001).

<sup>64</sup> See Daniel R. Faber & Eric J. Krieg, *Unequal Exposure to Ecological Hazards: Environmental Justice in the Commonwealth of Massachusetts* vi (2002), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1241174/>; Robert D. Bullard, *Dumping in Dixie: Race, Class, and Environmental Quality* 98, n.12–17 (3d ed. 2000).

<sup>65</sup> See also Vicki Been & Francis Gupta, *Coming to the Nuisance or Going to the Barrios? A Longitudinal Analysis of Environmental Justice Claims*, 24 Ecology L.Q. 1, 34 (1997), <https://www.jstor.org/stable/24113440>; Paul Mohai & Robin Saha, *Racial Inequality in the Distribution of Hazardous Waste: A National-Level Reassessment*, 54 Soc. Probs. 343, 361 (2007), <https://www.jstor.org/stable/10.1525/sp.2007.54.3.343>.

<sup>66</sup> See, e.g., Seema Arora & Timothy N. Cason, *Do Community Characteristics Influence Environmental Outcomes? Evidence from the Toxics Release Inventory*, 1 J. App. Econ. 413, 415–16 (1998).

<sup>67</sup> See, e.g., Lara P. Clark et al., *National Patterns in Environmental Injustice and Inequality: Outdoor NO<sub>2</sub> Air Pollution in the United States*, 9 PLOS ONE e94431, 2 (2014), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3988057/pdf/pone.0094431.pdf> (“reducing NO<sub>2</sub> concentrations to levels experienced by whites . . . for all nonwhites” would prevent 7,000 deaths per year from ischemic heart disease); Marie Lynn Miranda et al., *Making the Environmental Justice Grade: The Relative Burden of Air Pollution Exposure in the United States*, 8 Int’l J. Env’t Res. Pub. Health 1755, 1768–69 (2011), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3137995/pdf/ijerph-08-01755.pdf>.

<sup>68</sup> See Rachel D. Godsil, *Environmental Justice and the Integration Ideal*, 49 N.Y.L. Sch. L. Rev. 1109, 1120 (2005); Bullard, *supra* note 64, at 98–99.

Grave public health impacts—including asthma,<sup>69</sup> cancer,<sup>70</sup> and infant mortality,<sup>71</sup> as well as psychosocial phenomena like violent crime and post-traumatic stress disorder<sup>72</sup>—are now widely viewed as environmentally mediated consequences of residential segregation.<sup>73</sup>

### **C. The history of surveillance is inextricably intertwined with white supremacy.**

Surveillance technologies today arose in conjunction with state surveillance practices and policing with white supremacist origins—the subjugation of Black people. “The historical formation of surveillance is not outside of the historical formation of slavery.”<sup>74</sup> As leading privacy scholar Alan Westin noted half a century ago, “political fundamentalism has been a major limiting force on privacy in American culture. In one sense this is our nativist tradition, with its elements of xenophobia, religious and racial prejudice, and isolationism.”<sup>75</sup>

“As early as the seventeenth century, whites were constantly surveilling Black people. Slaves (and free Blacks) were observed closely in order to detect, prevent,

---

<sup>69</sup> See, e.g., Joint Ctr. for Pol. & Econ. Studies, *Breathing Easier: Community-Based Strategies to Prevent Asthma 2* (2004); Evalyn N. Grant et al., *The Relation of Socioeconomic Factors and Racial/Ethnic Differences in US Asthma Mortality*, 90 *Am. J. Pub. Health* 1923, 1925 (2000).

<sup>70</sup> See, e.g., U.S. Dep’t of Health & Human Servs., *Healthy People 2030: Discrimination*, <https://health.gov/healthypeople/priority-areas/social-determinants-health/literature-summaries/discrimination#top> (last visited Nov. 2, 2022).

<sup>71</sup> See *id.* (noting that infant mortality in Black population is almost double the national rate); see also Rachel Morello-Frosch & Russ Lopez, *The Riskscape and the Color Line: Examining the Role of Segregation in Environmental Health Disparities*, 102 *Env’t Res.* 181, 190–91 (2006).

<sup>72</sup> See, e.g., Magdalena Cerdá et al., *Addressing Population Health and Health Inequalities: The Role of Fundamental Causes*, 104 *Am. J. Pub. Health* S609, S610 (2014), <http://ajph.aphapublications.org/doi/pdf/10.2105/AJPH.2014.302055>.

<sup>73</sup> See, e.g., David R. Williams & Chiquita Collins, *Racial Residential Segregation: A Fundamental Cause of Racial Disparities in Health*, 116 *Pub. Health Reps.* 404, 409 (2001), <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1497358/pdf/12042604.pdf>; Masayoshi Oka & David W.S. Wong, *Capturing the two dimensions of residential segregation at the neighborhood level for health research*, 2 *Frontiers Pub. Health* 1, 12 (2014), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4142636/pdf/fpubh-02-00118.pdf>.

<sup>74</sup> Simone Browne, *Dark Matters: On the Surveillance of Blackness* 50 (Duke Univ. Press 2015); see also *id.* at 51 (discussing plantation rules for surveilling slaves).

<sup>75</sup> Alan Westin, *Privacy and Freedom* 28 (Atheneum 1967).

investigate, and prosecute Black misconduct, whether serious or minor.”<sup>76</sup> In colonial New York, “lantern laws” dictated that Black people walking at night either had to be accompanied by a white person or carry a lantern so that they “may be plainly seen.”<sup>77</sup> An early form of identification document was the slave pass required to travel off of a southern plantation, which had to be shown to slave patrols to avoid arrest or attack.<sup>78</sup> These slave patrols were used to control and terrorize Black people and were an early form of law enforcement in the South preceding many modern police forces.<sup>79</sup> Frederick Douglass wrote of the role of surveillance in slavery: “[A]t every gate through which we were to pass, we saw a watchman—at every ferry a guard—on every bridge a sentinel—and in every wood a patrol. We were hemmed in upon every side.”<sup>80</sup> Following the Civil War, slave patrols evolved into local police forces whose mission, in many cases, was to enforce Black Codes and Jim Crow.<sup>81</sup> Along the way, private commercial services and emerging technologies were used to surveil Black Americans. “Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.”<sup>82</sup>

Federal law enforcement has consistently surveilled Black leaders and activists. “At the turn of the 20<sup>th</sup> century, law enforcement targeted Ida B. Wells and Marcus Garvey as ‘race agitators.’”<sup>83</sup> The FBI, as part of its COINTELPRO operation spanning decades,

---

<sup>76</sup> Andrea Dennis, *Mass Surveillance and Black Legal History*, ACS Expert Forum (Feb. 18, 2020), <https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/>.

<sup>77</sup> Browne, *supra* note 74, at 25 (quoting New York ordinance); *id.* at 77–79.

<sup>78</sup> *Id.* at 52–53.

<sup>79</sup> See, e.g., Nat’l. L. Enf’t Officers Mem’l Fund, *Slave Patrols: An Early Form of American Policing*, <https://nleomf.org/slave-patrols-an-early-form-of-american-policing/> (last visited Nov. 15, 2022); Jill Lepore, *The Invention of the Police*, *The New Yorker* (July 13, 2020), <https://www.newyorker.com/magazine/2020/07/20/the-invention-of-the-police>; Gary Potter, *The History of Policing in the United States, Part 1*, Eastern Ky. Univ. Online (June 25, 2013), <https://ekuonline.eku.edu/blog/police-studies/the-history-of-policing-in-the-united-states-part-1/>.

<sup>80</sup> Frederick Douglass, *Narrative of the Life of Frederick Douglass, an American Slave. Written by Himself: Electronic Edition* 84–85 (1st ed. 1999), <https://docsouth.unc.edu/neh/douglass/douglass.html>.

<sup>81</sup> See Lepore, *supra* note 79.

<sup>82</sup> *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

<sup>83</sup> Nusrat Choudhury & Malkia Cyril, *The FBI Won’t Hand Over Its Surveillance Records on ‘Black Identity Extremists,’ so We’re Suing*, ACLU (Mar. 21, 2019),

surveilled Dr. Martin Luther King, Jr., Malcolm X, the Black Panthers, the Student Nonviolent Coordinating Committee, the Congress on Racial Equality, Duke Ellington, Louis Armstrong, and numerous other Black leaders, celebrities, activists, and clergy.<sup>84</sup> At the height of the Black Power movement, the FBI even targeted Black-owned bookstores.<sup>85</sup> Technology had a role to play in these events—the FBI’s attempts to sabotage Dr. King included “bugging his hotel rooms, photographic surveillance,” and using intercepted communications to attempt “to break up his marriage by sending selectively edited ‘personal moments he shared with friends and women’ to his wife.”<sup>86</sup> The National Security Agency likewise spied on the electronic communications of Dr. King and other activists as part of Project Minaret.<sup>87</sup>

During the Civil Rights Era, surveillance of civil rights activists was not just the province of the FBI; private actors and states were involved as well. For example, segregationist groups hired private investigators to wiretap clergy leading integration efforts and state anti-integration agencies bought off-the-shelf commercial technologies to surveil activists.<sup>88</sup> On behalf of a “Subversive Unit” that routinely used cameras and tape recorders to surveil civil rights events, Alabama state troopers photographed “virtually every white person who attended the funerals” of the four girls killed in the 1963 bombing of the 16<sup>th</sup> Street Baptist Church in Birmingham.<sup>89</sup> And, notably, one of the most important privacy and First Amendment cases in U.S. history, *NAACP v. Alabama*, arose from a segregationist government seeking disclosure of membership rolls identifying civil rights

---

<https://www.aclu.org/news/racial-justice/fbi-wont-hand-over-its-surveillance-records-black>.

<sup>84</sup> See Dennis, *supra* note 76; see also *Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 (Apr. 26, 1976) (“Church Committee Report”), [https://www.intelligence.senate.gov/sites/default/files/94755\\_II.pdf](https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf).

<sup>85</sup> Joshua Clark Davis, *The FBI’s War on Black-Owned Bookstores*, *The Atlantic* (Feb. 19, 2018), <https://www.theatlantic.com/politics/archive/2018/02/fbi-black-bookstores/553598/>.

<sup>86</sup> Dia Kayyali, *The History of Surveillance and the Black Community*, Elec. Frontier Found. (Feb. 13, 2014), <https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community>.

<sup>87</sup> Katelyn Epsley-Jones & Christina Frenzel, *The Church Committee Hearings & the FISA Court*, PBS Frontline (May 15, 2007), <https://www.pbs.org/wgbh/pages/frontline/home-front/preemption/churchfisa.html>.

<sup>88</sup> Westin, *supra* note 75, 115.

<sup>89</sup> Claude Sitton, *Alabama Compiling Files on Civil Rights Advocates*, *N.Y. Times*, Feb. 17, 1964, at 1, <https://www.nytimes.com/1964/02/17/archives/alabama-compiling-files-on-civil-rights-advocates.html>.

supporters.<sup>90</sup> It can reasonably be assumed that any commercial surveillance technology that can be used by or coopted by law enforcement to surveil marginalized groups *will* be used to surveil marginalized groups—“plac[ing] the liberty of every man in the hands of every petty officer.”<sup>91</sup> That is our history and practice.<sup>92</sup>

The origins of credit reporting bureaus are also intertwined with surveillance and discrimination. One of the first commercial credit bureaus, the Mercantile Agency, was founded in 1841 and its early reports “were incredibly subjective” and “were colored by the opinions of their predominantly white, male reporters, as well as their racial, class and gender biases.”<sup>93</sup> These firms invented credit systems to give “pseudo-scientific sleight of hand” to otherwise spurious reporting based on “private-sector mass surveillance.”<sup>94</sup> Mercantile Agency, for example, built its reports using “evaluations of people based on their racial background, gender and moral character.”<sup>95</sup> Similarly, consumer credit bureaus in the late 19<sup>th</sup> century “collected news of bankruptcies, divorces, lawsuits, and arrests. . . . And like commercial credit bureaus before them, they sought out prejudicial information about moral character, sometimes judging creditworthiness by what happened in the bedroom.”<sup>96</sup>

#### **D. Lack of diversity in tech, historically and today, affects system design.**

Addressing inequities in commercial data practices also requires a reckoning with the racist and sexist history of the tech sector that brought us step-by-step to this moment. During the early development of computer systems and networking technologies, Black

---

<sup>90</sup> *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449.

<sup>91</sup> *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) (quoting James Otis).

<sup>92</sup> Michael German, *The FBI Targets a New Generation of Black Activists*, Brennan Ctr. for Just. (June 26, 2020), <https://www.brennancenter.org/our-work/analysis-opinion/fbi-targets-new-generation-black-activists> (discussing FBI’s designation of “so-called ‘Black identity extremists’” and its surveillance of Black Lives Matter demonstrators, including “using its most advanced surveillance aircraft to monitor BLM protests in Baltimore after the police killing of Freddie Gray in 2018”).

<sup>93</sup> Sean Trainor, *The Long, Twisted History of Your Credit Score*, Time (July 22, 2015), <https://time.com/3961676/history-credit-scores/>.

<sup>94</sup> *Id.*

<sup>95</sup> Trina Paul, *When did credit scores start? A brief look at the long history behind credit reporting*, CNBC (Oct. 17, 2022), <https://www.cnbc.com/select/when-did-credit-scores-start/>.

<sup>96</sup> Sarah Jeong, *Credit Bureaus Were the NSA of the 19th Century*, The Atlantic (Apr. 21, 2016), <https://www.theatlantic.com/technology/archive/2016/04/mass-surveillance-was-invented-by-credit-bureaus/479226/>.

Americans, other people of color, and women were excluded from employment and educational opportunities in the field. There was an absence of these voices when pivotal choices were being made about computing architecture, design, and protocols. For example, in 1963–64, at the same time that the Massachusetts Institute of Technology was developing the “world’s first online community” as part of Project MAC for the Department of Defense,<sup>97</sup> the university’s Black enrollment was 0.5% of the student body.<sup>98</sup> MIT did not award a doctorate in computer science to a Black woman until 2001, to Latanya Sweeney. Dr. Sweeney pioneered the scientific field of data privacy through her groundbreaking research into deanonymization and privacy enhancing technologies and is a former Chief Technologist of the Commission.<sup>99</sup>

Many of our present problems related to privacy and data-driven discrimination could have been spotted and avoided if more diverse voices were in the room when computing systems were designed and the internet was conceived. Many inequities and security vulnerabilities were baked in because teams of predominantly white men failed to imagine how someone might maliciously or irrationally use information to harm another person.

This lack of diversity in the tech sector continues today. The United States population is 13.6% Black, 18.9% Latinx, and 2.9% multiracial.<sup>100</sup> However, diversity in the engineering, computer science, and technical workforces of major tech companies does not come close to looking like America:

- **Apple:** 5.5% of tech employees are Black, 7.8% are Latinx, and 2.4% are multiracial.<sup>101</sup>

---

<sup>97</sup> Def. Advanced Rsch. Projects Agency, *Project MAC* (last visited Nov. 2, 2022), <https://www.darpa.mil/about-us/timeline/project-mac>.

<sup>98</sup> Charlton D. McIlwain, *Black Software* 19–20 (Oxford Univ. Press 2020).

<sup>99</sup> See *Latanya Sweeney*, Harv. Kennedy Sch., <https://www.hks.harvard.edu/faculty/latanya-sweeney> (last visited Nov. 2, 2022); Latanya Sweeney, *Discrimination in Online Ad Delivery: Google ads, black names and white names, racial discrimination, and click advertising*, 11 ACM Queue 10–29 (2013), <https://dl.acm.org/doi/pdf/10.1145/2460276.2460278>; Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J.L., Med. & Ethics 98, 98–110 (1997), <https://latanyasweeney.org/JLME.pdf>.

<sup>100</sup> U.S. Census Bureau, *Quick Facts* (July 1, 2021), <https://www.census.gov/quick-facts/fact/table/US/PST045221>.

<sup>101</sup> Apple, *Inclusion & Diversity*, <https://www.apple.com/diversity/> (last visited Nov. 2, 2022).

- **Meta:** 2.4% of tech employees are Black, 4.8% are Latinx, and 3.1% are multiracial.<sup>102</sup>
- **Google:** 3.5% of tech employees are Black and 5.7% are Latinx.<sup>103</sup> 1.1% are Black women and 1.4% are Latinx women.<sup>104</sup> Google is the only company listed here that provides this intersectional data. More companies should share this valuable information.
- **Microsoft:** 4.4% of tech employees are Black, 5.8% Latinx, and 2.3% multiracial.<sup>105</sup>
- **Amazon:** 8.5% of corporate employees are Black, 8.7% are Latinx, and 3.2% are multiracial.<sup>106</sup> Amazon does not disambiguate tech vs. non-tech employees so it is difficult to get an accurate picture.

Until the products and services used by or on all of America are designed, tested, and built by people that reflect all of America, there will continue to be blind spots in their design.

### III. Commercial surveillance harms are prevalent, including discriminatory uses of personal data and related civil rights issues.

This section responds to many of the questions posed by the Commission to address the prevalence and harm of commercial surveillance practices that cause, contribute to, or exacerbate discrimination and other injuries to people of color. It provides examples in response to questions 3, 4, 55, and 66 in which the Commission asks which practices are prevalent and how they cause harm.<sup>107</sup> In response to questions 5 and 6, the examples will show that some of these harms are not easily discernible or quantifiable because a consumer cannot know when they were excluded from an opportunity because

---

<sup>102</sup> Maxine Williams, *Embracing Change Through Inclusion: Meta's 2022 Diversity Report*, Meta (July 19, 2022), <https://about.fb.com/news/2022/07/metas-diversity-report-2022/>.

<sup>103</sup> Google, *Google Diversity Annual Report 2022* 83 (2022), <https://about.google/belonging/diversity-annual-report/2022/>.

<sup>104</sup> *Id.*

<sup>105</sup> Microsoft, *Global Diversity & Inclusion Report* 13 (2021), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWNrak>.

<sup>106</sup> Amazon, *Our workforce data* (Dec. 31, 2021), <https://www.aboutamazon.com/news/workplace/our-workforce-data>.

<sup>107</sup> ANPR, 87 Fed. Reg. at 51281, 51283–84.

of discrimination—and thus cannot reasonably avoid the harm.<sup>108</sup> Harms to an individual may be difficult to measure but harms at the population level may be more readily quantifiable. The examples discussed below will address harms to different classes and in different sectors, in response to questions 12, 53, 57, and 65, and show the risks of inaction in response to questions 29 and 50.<sup>109</sup> These examples show the failures of self-regulation and need for Commission action, in response to questions 30 and 69.<sup>110</sup> Such action, as illustrated and discussed below, must consider harms to protected classes and other underserved groups, in response to question 68.<sup>111</sup>

Because of the far-reaching and persistent systemic effects of segregation and redlining, it is no surprise that discriminatory uses of personal data, as well as data practices that disproportionately disadvantage Black Americans and other communities of color, are prevalent in the online and data-driven economy. In this section we provide examples and documentation of these harms, with the caveat that a full accounting of the impact of commercial surveillance currently is not possible due to lack of transparency from companies using these tools. These harms are prevalent across sectors, including housing, employment, credit, insurance, healthcare, education, retail, and public accommodations. These harms manifest as economic discrimination;<sup>112</sup> through social media

---

<sup>108</sup> *Id.* at 51281; see also FTC, *Joint Statement of Chair Lina M. Khan, Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro M. Bedoya In the Matter of Passport Auto. Grp.*, FTC File No. 202 3199, at 3 (Oct. 18, 2022), [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) (hereinafter *Passport Auto. Grp. Statement*) (Black and Latino consumers could not reasonably avoid injury because “they typically had no way of knowing they were being charged more than their White counterparts”); FTC, *Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter In the Matter of Napleton Automotive Group*, FTC File No. 202 3195, at 3 (Mar. 31, 2022), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20Joined%20by%20RKS%20in%20re%20Napleton\\_Finalized.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20Joined%20by%20RKS%20in%20re%20Napleton_Finalized.pdf) (hereinafter *Napleton Statement*) (“[I]njuries stemming from disparate treatment or impact are unavoidable because affected consumers cannot change their status or otherwise influence the unfair practices.”).

<sup>109</sup> ANPR, 87 Fed. Reg. at 51281, 51283–84.

<sup>110</sup> *Id.* at 51282, 51284.

<sup>111</sup> *Id.* at 51284.

<sup>112</sup> See *Napleton Statement*, *supra* note 108, at 3; see also, e.g., *Passport Auto. Grp. Statement*, *supra* note 108.

as hate, harassment, and threats that chill free speech and equal opportunity;<sup>113</sup> and as voter intimidation and disinformation that disenfranchise Black and Brown voters. “Discrimination is not simply dollars and cents, hamburgers and movies; it is the humiliation, frustration, and embarrassment that a person must surely feel when he is told that he is unacceptable as a member of the public because of his race or color.”<sup>114</sup> The stigmatization caused by discrimination is itself a cognizable harm:

The right to equal treatment guaranteed by the Constitution is not co-extensive with any substantive rights to the benefits denied the party discriminated against. Rather, as we have repeatedly emphasized, discrimination itself, by perpetuating archaic and stereotypic notions or by stigmatizing members of the disfavored group as innately inferior and therefore as less worthy participants in the political community, can cause serious non-economic injuries to those persons who are personally denied equal treatment solely because of their membership in a disfavored group.<sup>115</sup>

In the context of commercial surveillance, these harms occur primarily in three ways. Either a company holding the personal data uses it to directly discriminate against people of color or other marginalized groups; a company holding the personal data makes it available to other actors who use it to discriminate; or 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>116</sup>

---

<sup>113</sup> See, e.g., Lindsay Mahowald, *LGBTQ People of Color Encounter Heightened Discrimination*, Ctr. for Am. Progress (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 that they do not experience discrimination: 36% report avoiding public spaces like stores or restaurants and 21% report avoiding getting necessary services for themselves or their families or avoiding travel to not experience discrimination).

<sup>114</sup> *Heart of Atlanta Motel*, 379 U.S. at 292 (1964) (Goldberg, J., concurring) (quoting S. Rep. No. 872, 88th Cong., 2d Sess., 16).

<sup>115</sup> *Heckler v. Mathews*, 465 U.S. 728, 739–40 (1984) (cleaned up).

<sup>116</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

Below, we provide evidence of the prevalence of the substantial injuries caused by commercial surveillance practices related to (A) housing, (B), employment, (C) credit and finance, (D) insurance, (E) public health and healthcare, (F) education, (G) public accommodations, (H) online hate, harassment, and threats, (I) voter intimidation and election disinformation, (J) government benefits and services, and (K) policing and law enforcement access to commercial surveillance. The common denominator in these examples is the sloppy or abusive use of personal data. By prohibiting discriminatory data use, 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.

## A. Housing

- Mortgage approval algorithms denied applications from homebuyers of color substantially more than white homebuyers. A review of over two million conventional mortgage applications found that, nationally, “lenders were 40 percent more likely to turn down Latino applicants for loans, 50 percent more likely to deny Asian/Pacific Islander applicants, and 70 percent more like to deny Native American applicants than similar White applicants. Lenders were 80 percent more likely to reject Black applicants than similar White applicants.”<sup>117</sup> Lenders used formulas mandated by Fannie Mae and Freddie Mac, which were known to be detrimental to people of color.<sup>118</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

---

(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) (“Evidence has emerged, however, that suggests that the use of big data, algorithms, machine learning, and artificial intelligence in housing-related decisions can perpetuate patterns of discrimination and thwart the efficacy of our antidiscrimination laws.”); James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Detering 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).

<sup>117</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>118</sup> *Id.*

race and other protected characteristics—including literal redlining.<sup>119</sup> Facebook has also been sued by civil rights advocates for similar conduct and causes of action.<sup>120</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

---

<sup>119</sup> See U.S. Dep’t of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 21, 2022), <https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known>; Charge of Discrimination, *U.S. Dep’t of Hous. and Urban Dev. v. Facebook, Inc.*, FHEO No. 01-18-0323-8, at 4 (Mar. 28, 2019) (“[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.**”) (emphasis added); see also Brief of Amicus Curiae Lawyers’ Committee for Civil Rights Under Law in Support of Plaintiff’s Opposition to Facebook’s Demurrer to First Amended Complaint at 10, *Liapes v. Facebook, Inc.*, Case No. 30-CIV-01712 (Cal. Super. Ct. Mar. 5, 2021), <https://lawyerscommittee.org/wp-content/uploads/2021/03/Leave-and-Amicus-Combined.pdf> (showing screenshot of ad system redlining to exclude a ZIP code).

<sup>120</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>.

address the problem.<sup>121</sup> Facebook’s own civil rights auditors even called out the risk of algorithmic bias in its advertising system.<sup>122</sup>

- Google and Twitter have both been investigated by HUD for similarly discriminating in housing advertisements in violation of the Fair Housing Act.<sup>123</sup>

---

<sup>121</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.ap-news.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* (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*, Proc. of the 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>122</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>123</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), <https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/>.

- Landlords and other housing providers use social media targeted advertising tools to engage in discrimination on the basis of race, sex, and age.<sup>124</sup>
- Landlords use tenant screening and background check algorithmic systems that frequently produce flawed reports that cause denials of lease applications.<sup>125</sup> These oversimplified recommendation systems disproportionately impact Black and Latino tenants, making it harder for them to secure affordable housing.<sup>126</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>127</sup>
- 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>128</sup>

---

<sup>124</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>125</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>126</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>127</sup> Associated Press, *Redfin to pay \$4 million to settle lawsuit alleging housing discrimination* (May 2, 2022), <https://www.marketwatch.com/story/redfin-to-pay-4-million-to-settle-lawsuit-alleging-housing-discrimination-01651500520>.

<sup>128</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>.

## B. Employment

- A major report from Upturn found that algorithms used to automate parts of the hiring process can produce discriminatory outcomes. Predictive hiring tools play “a powerful role in determining who learns of open positions” but can “reproduce patterns of inequity at all stages of the hiring process, even when the tools explicitly ignore race, gender, age, and other protected attributes.”<sup>129</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>130</sup>
- 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>131</sup>
- Amazon previously used a machine learning tool to assess job applicants for technical positions, but it systematically discriminated in favor of men.<sup>132</sup>
- Algorithms are becoming more common tools to aid human resources departments for recruitment and development, but there are concerns that these tools can

---

<sup>129</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>130</sup> See Avi Asher-Schapiro, *ANALYSIS—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>.

<sup>131</sup> See 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/> (ads for truck drivers were shown overwhelmingly to men while ads for child care workers were shown overwhelmingly to women).

<sup>132</sup> Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters (Oct. 10, 2018), <https://www.reuters.com/article/us-amazon-com-jobs-automation-insightidUSKCN1MK08G>.

contribute to discrimination.<sup>133</sup> These “bossware” tools are being sold to government agencies as well.<sup>134</sup>

- Employee surveillance tools deployed during the pandemic to monitor remote workers are very invasive and likely to persist beyond the pandemic.<sup>135</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>136</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>137</sup>
- 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>138</sup>

### C. Credit and finance

- One study found that lenders charge otherwise equivalent Black and Latino borrowers higher rates—7.9 basis points higher for purchase mortgages and 3.6 basis points higher for refinance mortgages. This is estimated to cost these borrowers \$765 million

---

<sup>133</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>134</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>135</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>136</sup> *Id.*

<sup>137</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/>.

<sup>138</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/>.

per year in extra interest. Algorithms used by FinTech lenders are less discriminatory than face-to-face lending—but are still discriminatory.<sup>139</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 re-finance loans, amounting to \$250–\$500 million annually.<sup>140</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>141</sup>
- Lax data security at credit reporting agencies such as Experian<sup>142</sup> and Equifax<sup>143</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; low-income consumers are also less likely to have the resources to bounce back after being ripped off.<sup>144</sup>

---

<sup>139</sup> See Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era* (Nat’l Bureau Econ. Res. Working Paper No. 25943, 2019), <https://www.nber.org/papers/w25943>.

<sup>140</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>141</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>142</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>143</sup> See FTC, *Equifax, Inc.*, FTC File No. 172 3203, No. 1:19-cv-03297-TWT (July 31, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc>.

<sup>144</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), <https://www.ftc.gov/system/files/documents/reports/serving-communities-color>

- 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>145</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>146</sup>
- Data used to score consumers’ credit has been shown to be capable of predicting the race and gender of loan applicants.<sup>147</sup>

#### D. Insurance

- Health insurance companies buy information from data brokers to predict costs of patient health care, including demographic and lifestyle data, which can result in higher rates for consumers of color. As an insurance salesman joked, “God forbid you live on the wrong street these days. You’re going to get lumped in with a lot of bad things.”<sup>148</sup>

---

[staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report\\_oct\\_2021-508-v2.pdf](#) (hereinafter *Serving Communities of Color*); 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>145</sup> Aaron Reike & Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, Upturn (Oct. 2015), <https://www.upturn.org/reports/2015/led-astray/>.

<sup>146</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>147</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>148</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>.

All forms of insurance are now “adjusting premiums and policies based on new forms of surveillance.”<sup>149</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>150</sup> Insurance premiums are set by actuarial algorithms using many non-driving factors, which contributes to higher rates in Black neighborhoods.<sup>151</sup> These insurance formulas also charge higher premiums to individuals with less education or lower-paying jobs.<sup>152</sup> “[C]onfounding scoring algorithms” judge applicants “less on driving habits and increasingly on socio-economic factors.”<sup>153</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>154</sup> which would have contributed to discriminatory higher premiums routinely

---

<sup>149</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>150</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>151</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>.

<sup>152</sup> See 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>153</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>154</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>.

paid by consumers of color who often lack competitive options for insurance. The Allstate personalized pricing algorithm was still implemented in other states.<sup>155</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 as driver name, driver fatigue, driver heartrate, and the language used on a dashboard display.<sup>156</sup> The companies use this data in usage-based insurance, which charges higher premiums to “risky drivers.”<sup>157</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 insureds.<sup>158</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.

#### **E. Public health and healthcare**

- Social media news feed algorithms and advertising systems significantly contribute to the amplification of health disinformation about COVID-19.<sup>159</sup> In the first months of the

---

<sup>155</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>156</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> (last visited Nov. 7, 2022) (click an item in the menu and then click “Open Airtable” to see the Full Data Catalog for that item).

<sup>157</sup> Keegan & Ng, *supra* note 156.

<sup>158</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>159</sup> See Virginia Alvino Young, *Nearly Half of the Twitter Accounts Discussing ‘Reopening America’ May Be Bots*, Carnegie Mellon Univ. (May 27, 2020),

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 the 10 leading health institutions, such as the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC).”<sup>160</sup> Public health agencies have faced particular difficulties getting their paid public service announcements to reach Black social media users.<sup>161</sup> The effects of this disparity in reach has real-life consequences, as COVID disproportionately harms Black and Hispanic Americans, who experience higher disease prevalence, hospitalization, and mortality compared to whites and who have less access to healthcare as a consequence of systemic racism.<sup>162</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, Black patients appeared to be sicker than white patients.<sup>163</sup> Another algorithm made “wildly irrational” decisions depriving necessary care to people with disabilities.<sup>164</sup>
- Social media, particularly Instagram, push content to teenage girls that is known to be harmful to their physical and mental health, because it maximizes user

---

<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>160</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>161</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>.

<sup>162</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>163</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 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>164</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>.

engagement.<sup>165</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>166</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>167</sup> When teens engaged in suicidal ideation, 6% of them traced it to Instagram.<sup>168</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>169</sup> People of color are less likely to have access to specialty medical care,<sup>170</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>171</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>172</sup> Access to reproductive healthcare is essential for Black women and low-income women, who experience

---

<sup>165</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>166</sup> *Id.*

<sup>167</sup> *Id.*

<sup>168</sup> *Id.*

<sup>169</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>170</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>171</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>172</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>.

higher rates of unintended pregnancy and are more likely to have abortions.<sup>173</sup> Consequently, surveillance of people seeking reproductive healthcare is likely to disproportionately impact these populations.

- Facebook gave Nebraska law enforcement, in response to a court order, the private communications and other private data of a teenager who sought medication for an at-home abortion.<sup>174</sup> Facebook has collected sensitive patient information from healthcare and hospital websites, including data on people seeking abortions and children.<sup>175</sup> It collected health information, including ovulation data, from health apps without user consent.<sup>176</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>177</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.

---

<sup>173</sup> See Katherine Kortsmitt et al., *Abortion Surveillance – United States, 2018*, Ctrs. for Disease Control & Prevention 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., at 11 (2016), <https://www.guttmacher.org/report/characteristics-us-abortion-patients-2014>.

<sup>174</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>175</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>176</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>177</sup> Gioacchino Tangari et al., *Mobile health and privacy: cross sectional study*, BMJ (June 17, 2021), <https://www.bmj.com/content/373/bmj.n1248>.

- Data brokers also sell personal data to health care providers, including “criminal records, online purchasing histories, retail loyalty programs and voter registration data.”<sup>178</sup> These data can be fed into algorithms used to classify patients’ health risks and can produce biases if not handled correctly.<sup>179</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>180</sup>
- Poorly designed medical research can lead to procedures or technologies that misdiagnose patients. One recent 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>181</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>182</sup>

## F. Education

- Online and for-profit colleges specifically target Black and Latino prospective students with predatory marketing practices while providing low-quality education and high debt loads.<sup>183</sup>

---

<sup>178</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>179</sup> See Obermeyer, *supra* note 163.

<sup>180</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>181</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>182</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>183</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-*

- 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>184</sup>
- Higher education institutions are increasingly adopting “student success analytics” intended to aid students in their studies.<sup>185</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>186</sup> Black students were deemed “higher risk for failure” as much as four times as often as white peers.<sup>187</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>188</sup> Enrollment algorithms often discriminate against people of color and women.<sup>189</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>190</sup>

---

*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>184</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>.

<sup>185</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>186</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>187</sup> *Id.*

<sup>188</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>189</sup> *Id.*

<sup>190</sup> Douglas MacMillan & Nick Anderson, *Student tracking, secret scores: How college admissions offices rank prospects before they apply*, Wash. Post (Oct. 14, 2019),

More than 75 percent of colleges and universities uses analytics in admissions decisions.<sup>191</sup>

- Naviance college admissions software, used by 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>192</sup>
- Surveillance of students disproportionately harms Black and Brown students.<sup>193</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>194</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>195</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

---

<https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/>.

<sup>191</sup> Ronald Yanosky & Pam Arroway, *The Analytics Landscape of Higher Education, 2015*, Educause, at 17 (2015) <https://library.educause.edu/~media/files/library/2015/5/ers1504cl.pdf>.

<sup>192</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>.

<sup>193</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>194</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>195</sup> *Id.*

students from marginalized groups” despite evidence that students of color face disparities in discipline.<sup>196</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>197</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>198</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>199</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 messages, photos, app data, location data, and other communications.<sup>200</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>201</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

---

<sup>196</sup> 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>197</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-a2j3vstyijhhj36n57ri5zdhi-story.html>.

<sup>198</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/facial-recognition-company-lied-to-school-district-about-its-racist-tech>.

<sup>199</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/>.

<sup>200</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>201</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>.

facial recognition to track students' actions.<sup>202</sup> Black women, in particular, are at greater risk of being falsely accused of cheating by these automated tools.<sup>203</sup>

### G. Public accommodations

- The Social Media Victims Law Center filed a lawsuit against YouTube, Meta, and TikTok, alleging that their content recommendation engines engage in racial profiling and disproportionately push violent, drug-filled, and sexual content to Black youth, including content driving Black kids to engage in self-harm.<sup>204</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>205</sup>
- Google blocked YouTube advertisers from being able to target ads to “Black Lives Matter” and “Black Power” but allowed ad targeting 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>206</sup> This undermines 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.

---

<sup>202</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>203</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>204</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>.

<sup>205</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>.

<sup>206</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>.

- Google’s ad portal returned pornographic suggestions as its top results to 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. In addition, by 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>207</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>208</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>209</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 executives received those data, they halted further research into racial bias in the system.<sup>210</sup>

---

<sup>207</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>208</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>209</sup> See *Serving Communities of Color*, *supra* note 144, 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/>.

<sup>210</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>.

- 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>211</sup>
- Algorithms that distribute discount-related ads tend to direct those ads toward high-income white users.<sup>212</sup> An algorithm calibrated to send an ad featuring a sale would recognize that high-income white people are historically more able to time discretionary purchases to price discounts and therefore more likely to respond to a price discount.<sup>213</sup> The algorithm would then reinforce the disparity by further sending the ad to additional white users, because the algorithm is programmed to maximize responsiveness.<sup>214</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>215</sup>
- Leading automated speech recognition software from Amazon, Apple, Google, IBM, and Microsoft are all less accurate when processing the speech of Black Americans. These speech recognition systems are used in a wide variety of commercial settings, including automated closed captioning, dictation in healthcare settings, and virtual assistants like Siri.<sup>216</sup>

---

<sup>211</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>212</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>213</sup> *Id.*

<sup>214</sup> *Id.*

<sup>215</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>216</sup> Allison Koenecke et al., *Racial disparities in automated speech recognition*, 117 PNAS 7684 (2020), <https://www.pnas.org/doi/10.1073/pnas.1915768117>.

- Black influencers drive popular trends on TikTok but do not equitably share in the profits created by their monetized content.<sup>217</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>218</sup>

#### H. Online hate, harassment, and threats

- Over 40% of U.S. adults have personally experienced online harassment, largely through social media.<sup>219</sup> Half of Black and Hispanic targets of online harassment say they were targeted because of their race or ethnicity, compared to 17% of white targets.<sup>220</sup> 25% of all adults have experienced stalking, physical threats, sustained harassment, or sexual harassment—and that number rises to 51% for lesbian, gay, or bisexual adults.<sup>221</sup> 64% of adults under age 30 have experienced online harassment.<sup>222</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>223</sup>

---

<sup>217</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>218</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>219</sup> See Emily A. Vogels, *The State of Online Harassment*, Pew Rsch. Center (Jan. 13, 2021), <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>.

<sup>220</sup> *Id.*

<sup>221</sup> *Id.*

<sup>222</sup> *Id.*

<sup>223</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).

- Platform algorithms help white supremacists connect with each other and systematically promote divisive material in the pursuit of maximizing user engagement.<sup>224</sup> An internal Facebook study noted that “64% of extremist group joins are due to our recommendation tools . . . our recommendation systems grow the problem.”<sup>225</sup> It 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>226</sup> When these issues were raised to Facebook executives, they declined to make changes.<sup>227</sup>
- YouTube video recommendations systematically recommend harmful and progressively more extreme content to viewers, creating pathways to white supremacy and hate group recruitment.<sup>228</sup>
- Following the murder of George Floyd by Minneapolis police, racist disinformation about his death surged on Facebook, YouTube, and Twitter.<sup>229</sup>

---

<sup>224</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>225</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>226</sup> *Id.*

<sup>227</sup> *See id.*

<sup>228</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>229</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>.

- Language models and other AI trained on large real world data sets capture and reproduce racist stereotypes and biases.<sup>230</sup> Hateful autocomplete recommendations in Google Search is one highly visible manifestation of this problem.<sup>231</sup> As is Google's photo-categorization software labeling Black people as gorillas, which Google failed to fix for years.<sup>232</sup>
- Facebook profits from running ads on searches for hate group pages.<sup>233</sup> Google's ad network has been manipulated to help monetize websites that promote violence and misinformation.<sup>234</sup> Both have previously allowed ad targeting based on racism and hate speech.<sup>235</sup>
- Commercial surveillance tools are used by domestic abusers and stalkers to track, threaten, and harm their targets. "Privacy is about power, and undermining privacy serves the powerful at the cost of the powerless, even at home. For an unknown number of people, surveillance is not an exotic threat, a national story, a geopolitical game. For them, surveillance begins at home."<sup>236</sup>

---

<sup>230</sup> See Moin Nadeem et al., *StereoSet: Measuring stereotypical bias in pretrained language models* in *Proc. of the 59th Ann. Meeting of the Ass'n for Computational Linguistics and the 11th Int'l Joint Conf. on Nat. Language Processing* 5356–5371 (2021), <https://arxiv.org/pdf/2004.09456.pdf>.

<sup>231</sup> Issie Lapowsky, *Google Autocomplete Still Makes Vile Suggestions*, *Wired* (Feb. 12, 2018), <https://www.wired.com/story/google-autocomplete-vile-suggestions/>.

<sup>232</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>233</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>234</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>235</sup> See Sapna Maheshwari & Alexandra Stevenson, *Google and Facebook Face Criticism for Ads Targeting Racist Sentiments*, *N.Y. Times* (Sept. 15, 2017), <https://www.ny-times.com/2017/09/15/business/facebook-advertising-anti-semitism.html>.

<sup>236</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/?sh=1c0161087f41>.

- An AI chatbot developed by Google was racist and the company did not adequately invest in diversity or AI ethics, according to a fired engineer.<sup>237</sup>
- Facebook was instrumental in enabling the genocide of Rohingya Muslims in Myanmar.<sup>238</sup> The United Nations observed that Facebook played a significant role in the genocide.<sup>239</sup> The role of Facebook in Myanmar echoes the way in which radio stations incited the Rwandan Genocide in the 1990s.<sup>240</sup>
- 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>241</sup>
- Facebook allowed ads to run in Kenya that promoted ethnic cleansing in the run-up to a national election.<sup>242</sup>
- Following the May 14, 2022 attack on the Black community in Buffalo that left ten Black people dead, the Office of the New York State Attorney General published an investigative report on the role of online platforms in the mass shooting. The office

---

<sup>237</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'*, Insider (July 31, 2022), <https://www.businessinsider.com/google-engineer-blake-lemoine-ai-ethics-lambda-racist-2022-7>.

<sup>238</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>.

<sup>239</sup> See 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>.

<sup>240</sup> See, e.g., Meghan Lyon, *Radio in the Rwandan Genocide*, Duke Univ. Librs. (May 10, 2013), <https://blogs.library.duke.edu/rubenstein/2013/05/10/radio-in-the-rwandan-genocide/>.

<sup>241</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>242</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>.

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>243</sup>

### I. 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>244</sup> They spent only \$1,000 on the robocalls.<sup>245</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>246</sup>

---

<sup>243</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>244</sup> See *Nat’l Coal. on Black Civic Participation v. Wohl*, 498 F. Supp. 3d 457 (S.D.N.Y. 2020).

<sup>245</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>246</sup> *Nat’l Coal. on Black Civic Participation*, 498 F. Supp. 3d at 464.

- The Russian government used social media platforms 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>247</sup> The campaign also used racially divisive issues in targeted ads.<sup>248</sup> Foreign adversaries used conventional advertising and targeting tools on social media,<sup>249</sup> showing the dangerous ways targeted advertising tools can be abused.<sup>250</sup>
- Social media plays a key role in disinformation campaigns that spread conspiracy theories and seek to undermine election integrity.<sup>251</sup> The structure of the platforms, their profiling of users, and the use of recommendation engines to maximize user engagement at all costs creates a perfect storm for the spread of disinformation and disenfranchisement.<sup>252</sup> “[T]o tackle thorny issues like misinformation, [Facebook employees] often had to demonstrate that their proposed solutions wouldn’t anger powerful partisans or come at the expense of Facebook’s growth.”<sup>253</sup>

---

<sup>247</sup> See S. Rep. No. 42-193, <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>.

<sup>248</sup> See Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, U.S. S. Select Comm. on Intel. (Oct. 2019), <https://digitalcommons.unl.edu/senatedocs/2/>.

<sup>249</sup> See 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>250</sup> See Craig Silverman, *Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months*, ProPublica: Tech. (July 1, 2022), <https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine>.

<sup>251</sup> See Election Integrity P’ship, *The Long Fuse: Misinformation and the 2020 Election* (2021), <https://www.eipartnership.net/report>.

<sup>252</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>253</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>.

- 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>254</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>255</sup> culminating in the violent attack on the U.S. Capitol on January 6, 2021.<sup>256</sup> However, 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>257</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 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>258</sup> The number of Black voters in the “deterrence” 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

---

<sup>254</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>255</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>256</sup> See generally Ryan Goodman & Justin Hendrix, *January 6 Clearinghouse*, Just Sec. (Sept. 7, 2022), <https://www.justsecurity.org/77022/january-6-clearinghouse/> (collecting primary and secondary source materials related to the Big Lie and attack on the Capitol).

<sup>257</sup> See 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>.

<sup>258</sup> Channel 4 News Investigations Team, *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016* (Sept. 28, 2020), <https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016>.

campaign is unknown because there was no transparency as to what ads were sent to whom.<sup>259</sup>

- Disinformation on social media in non-English languages, particularly Spanish, was rampant in the 2020 election cycle and continues to be a major problem.<sup>260</sup> For example, Facebook ads targeting Hispanic populations inaccurately described prominent American politicians as “communist” and compared them to socialist presidents in South America.<sup>261</sup>
- Users searching Google 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>262</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>263</sup>

---

<sup>259</sup> *Id.*

<sup>260</sup> See 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>.

<sup>261</sup> See Amanda Seitz & Will Weissert, *Inside the ‘big wave’ of misinformation targeted at Latinos*, AP News, (Dec. 1, 2021), <https://apnews.com/article/latinos-misinformation-election-334d779a4ec41aa0eef9ea80636f9595>.

<sup>262</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>263</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/>.

- Meta developed an AI chatbot and within a few days of studying online chatter, it began spreading election denialism and spreading anti-Semitic conspiracy theories.<sup>264</sup>

## J. Government benefits and services

- Automated decision-making systems have erroneously disqualified individuals from food assistance benefits using a vague “criminal justice disqualification” criterion.<sup>265</sup> An algorithmic tool used by the Michigan Unemployment Insurance Agency to identify fraud in applications for unemployment benefits similarly incorrectly disqualified applicants.<sup>266</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 incorrect denials of benefits, particularly in communities of color.<sup>267</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 recently shelved a plan to use it for tax filings.<sup>268</sup>

## K. Policing and law enforcement access to commercial surveillance

- Software developed and sold to law enforcement and courts for so-called “predictive policing,” risk assessments, and criminal sentencing has been shown time and again to be racially biased against Black Americans.<sup>269</sup> Many jurisdictions use algorithms to predict recidivism risk when setting probation conditions, with little transparency as to

---

<sup>264</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>265</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/litigatingalgorithms-2019-us.pdf>.

<sup>266</sup> *Id.*

<sup>267</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>268</sup> See *infra* § VI.C.1.

<sup>269</sup> See Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

the formulas and criteria considered.<sup>270</sup> The American Bar Association passed a resolution urging that pretrial risk assessment tools should not be used unless they can be proven to be unbiased.<sup>271</sup>

- Reliance on arrest records to train algorithms reproduces discrimination. An investigation of a predictive policing tool deployed in Oakland, California found that it 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>272</sup>
- Data brokers like LexisNexis collect and sell personal data to U.S. Immigration and Customs Enforcement, which can use this information to fuel immigration raids even in sanctuary jurisdictions.<sup>273</sup>
- Following the *Dobbs* decision overturning *Roe v. Wade*, data brokers refuse to stop collecting information on pregnant people, which could be used to prosecute people seeking abortions.<sup>274</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

---

<sup>270</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>.

<sup>271</sup> Lyle Moran, *Pretrial risk-assessment tools should only be used if they’re transparent and unbiased, warns ABA House*, ABA Journal (Feb. 14, 2022), <https://www.abajournal.com/news/article/resolution-700>.

<sup>272</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>273</sup> Madison Savedra, *Immigrant Rights Advocates Push Cook County to Find Out if ICE Is Using Data Brokers to Skirt Sanctuary City Ordinances*, Block Club Chi. (Aug. 3, 2022), <https://blockclubchicago.org/2022/08/03/immigrant-rights-advocates-push-cook-county-to-find-out-if-ice-is-using-data-brokers-to-skirt-sanctuary-city-ordinances/>.

<sup>274</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>.

organizations. Company insiders say it overamplified supposed criminal threats in a manner than amounted to racial profiling and stereotyping.<sup>275</sup>

- Amazon’s social media crime-reporting app, Neighbors, routinely facilitates in racial profiling, with people of color being reported as “suspicious.” It also has forums rife with racism.<sup>276</sup>
- Facebook, Twitter, and Instagram provided user data to Geofeedia, a social media monitoring product that had been marketed to law enforcement agencies to surveil civil rights activists.<sup>277</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>278</sup> to genealogy and DNA companies sharing genetic data with the FBI,<sup>279</sup> to federal agencies simply buying cell phone location data in bulk.<sup>280</sup>
- Even if an individual consents to share their own data in a manner that could expose it to law enforcement, they cannot consent for others. Yet many forms of data made

---

<sup>275</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>276</sup> Caroline Haskins, *Amazon’s Home Security Company Is Turning Everyone Into Cops*, *Vice: Motherboard* (Feb. 7, 2019), <https://www.vice.com/en/article/qvyvzd/amazon-home-security-company-is-turning-everyone-into-cops>.

<sup>277</sup> Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, *ACLU of N. Cal.* (Oct. 11, 2016), <https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target>.

<sup>278</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-quests-ice-officials-say-now-it-owes-them-million/>.

<sup>279</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>280</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/jgxx3g/secret-service-phone-location-data-babel-street>.

available—including contacts, addresses, genetic information, and associations—necessarily impinge the privacy of others as well, without their knowledge or consent.

\* \* \*

The examples above are merely a subset of the commercial surveillance practices that are prevalent and harmful to Black Americans and other communities of color.

[W]hen these technical codes move beyond the bounds of the carceral system, beyond labeling people as “high” and “low” risk criminals, when automated systems from employment, education, healthcare, and housing come to make decisions about people’s deservedness for all kinds of opportunities, then tech designers are erecting a digital caste system, structured by existing racial inequities that are not just colorblind[.] These tech advances are sold as morally superior because they purport to rise above human bias, even though they could not exist without data produced through histories of exclusion and discrimination.<sup>281</sup>

Commercial surveillance is derived from and reinforces structural racism. The question remaining is what the Commission will do about it.

#### **IV. Discrimination is an unfair and deceptive trade practice.**

Discrimination is the quintessential unfair practice. The FTC Act looks to public policy when considering whether an act or practice is unfair.<sup>282</sup> It is the well-established public policy of the United States that invidious discrimination on the basis of race, sex, and other immutable characteristics is unfair, unlawful, and must be eradicated. This

---

<sup>281</sup> Benjamin, *supra* note 3, at 10.

<sup>282</sup> See 15 U.S.C. § 45(n) (“In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence.”).

promise is the original intent of America, persistently declared<sup>283</sup> but never fully realized.<sup>284</sup>

Since 1866, racial discrimination in commerce has been unlawful.<sup>285</sup> Since 1868, all people have been entitled to equal protection of the laws.<sup>286</sup> Since 1954, separate-but-equal segregation has been prohibited.<sup>287</sup> And over the past 60 years, Congress has repeatedly reaffirmed this core public policy through civil rights legislation prohibiting discrimination in public accommodations, housing, insurance, employment, credit, education, federally-funded programs, and many other areas of commerce.<sup>288</sup>

In questions 10, 12, 39, 40, 60, 67, 71 of the ANPR, the Commission asks how it should treat commercial surveillance practices that are discriminatory.<sup>289</sup> They should be prohibited as unfair and deceptive trade practices in violation of Section 5 of the FTC Act. This prohibition must apply to both intentional discrimination and discrimination by disparate impact—both are unfair and within the scope of the Act. Discrimination causes substantial injury to consumers, is not reasonably avoidable, and does not have

---

<sup>283</sup> *The Declaration of Independence* para. 2 (U.S. 1776) (“We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the pursuit of Happiness.”).

<sup>284</sup> See Frederick Douglass, *Oration, Delivered in Corinthian Hall, Rochester* (July 5, 1852), <https://rbscp.lib.rochester.edu/2945> (“The rich inheritance of justice, liberty, prosperity and independence, bequeathed by your fathers, is shared by you, not by me. . . . This Fourth of July is *yours*, not *mine*. *You* may rejoice, I must mourn. To drag a man in fetters into the grand illuminated temple of liberty, and call upon him to join you in joyous anthems, were inhuman mockery and sacrilegious irony.” (emphasis in original)).

<sup>285</sup> See Civil Rights Act of 1866 § 1, 42 U.S.C. §§ 1981, 1982.

<sup>286</sup> See U.S. Const. amend. XIV (“No State shall . . . deny to any person within its jurisdiction the equal protection of the laws.”).

<sup>287</sup> *Brown v. Bd. of Educ. of Topeka*, 347 U.S. 483, 495 (1954).

<sup>288</sup> See, e.g., The Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241 (codified as amended in scattered sections of 42 U.S.C.); Americans with Disabilities Act, 42 U.S.C. § 12101 *et seq.*; Fair Housing Act of 1968, Pub. L. No. 90-284, 82 Stat. 73 (codified at scattered sections of 18, 25, 42 U.S.C.); Home Mortgage Disclosure Act, 12 U.S.C. §§ 461, 2801 *et seq.*; Affordable Care Act § 1557, 42 U.S.C. § 18116; Age Discrimination in Employment Act, 29 U.S.C. § 621 *et seq.*; Equal Pay Act of 1963; Pregnancy Discrimination Act, Pub. L. No. 95-555 (amending 42 U.S.C. § 2000e *et seq.*); Civil Rights Act of 1991, Pub. L. No. 102-166 (amending 42 U.S.C. § 1981 *et seq.*); Equal Credit Opportunity Act, 15 U.S.C. § 1961 *et seq.*; Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x; Title IX of the Education Amendments of 1972, 20 U.S.C. § 1681–1688.

<sup>289</sup> See ANPR, 87 Fed. Reg. at 51281, 51283–84.

countervailing benefits.<sup>290</sup> And, as discussed above, discrimination in commercial surveillance practices is prevalent.<sup>291</sup>

In this section we (1) show that discrimination is an unfair trade practice; (2) show that discrimination, if undisclosed, is a deceptive trade practice; (3) establish that the FTC Act applies to both disparate treatment and disparate impact; and (4) discuss the immutable traits that the Commission should designate as protected characteristics.

### **A. Discrimination is an unfair trade practice.**

The FTC Act declares that “unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.”<sup>292</sup> Under the Act, the Commission is not just “empowered” but “*directed* to prevent persons . . . from using . . . unfair or deceptive acts or practices in or affecting commerce.”<sup>293</sup> An act or practice is unfair if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”<sup>294</sup> The FTC “may pursue an unfair practice even if the practice is facilitated by violations of a law not administered by the FTC . . . .”<sup>295</sup>

Discrimination on the basis of protected characteristics falls within the plain and unambiguous text of the FTC Act, satisfying the three-part test of the Unfairness Doctrine. Consequently, the Act requires the Commission to prevent firms from engaging in this unfair trade practice.<sup>296</sup> The Commission can meet this mandate by issuing and enforcing a rule prohibiting discrimination.<sup>297</sup>

#### **1. Discrimination causes substantial injury to consumers.**

As catalogued extensively above,<sup>298</sup> racial segregation, redlining, and other forms of invidious discrimination have caused immense and long-lasting harms to Black Americans and others who are adversely affected by disparate treatment. Furthermore,

---

<sup>290</sup> See 15 U.S.C. § 45(n).

<sup>291</sup> See *supra* § III.

<sup>292</sup> 15 U.S.C. § 45(a)(1).

<sup>293</sup> *Id.* § 45(a)(2) (emphasis added).

<sup>294</sup> *Id.* § 45(n).

<sup>295</sup> *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1191 (10th Cir. 2009).

<sup>296</sup> *Id.* § 45(a)(2).

<sup>297</sup> See *id.* § 57a.

<sup>298</sup> See *supra* § II.

discrimination causes stigmatic and non-economic injuries to affected communities.<sup>299</sup> And again as catalogued extensively above,<sup>300</sup> commercial surveillance practices that are discriminatory result in severe harms to communities of color across every sector: housing, employment, credit and finance, insurance, public health and healthcare, education, public accommodations, voting rights, online hate, government benefits and services, and policing and law enforcement. “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>301</sup>

## **2. Consumers cannot reasonably avoid the harms of discrimination; the act of avoidance is itself harmful.**

Consumers cannot reasonably avoid the harms of discrimination. We agree with Chair Khan and Commissioner Slaughter that by definition a consumer cannot change their own immutable characteristics or otherwise influence a discriminatory practice.<sup>302</sup>

Discrimination is not a product feature touted on a box and weighed in the aisle of a marketplace. In the context of commercial surveillance, 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 ad networks or assessment tools for prospective employees—and those intermediaries may engage in discrimination. But even if a consumer knows that a service 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 automated decision-making tools even if they know it is unfair.<sup>303</sup> Similarly, in many settings one cannot avoid facial recognition—the technology can be used in any public place with surveillance cameras, by video doorbells pointed at a sidewalk, or by school or workplace surveillance

---

<sup>299</sup> *Heckler*, 465 U.S. at 739.

<sup>300</sup> See *supra* § III.

<sup>301</sup> Exec. Off. of the President, *supra* note 116; see also FTC, *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>302</sup> See *Napleton Statement*, *supra* note 108, at 3; see also *Passport Auto. Grp. Statement*, *supra* note 108, at 2.

<sup>303</sup> See *supra* § III.

software.<sup>304</sup> Or due to market concentration, a consumer may have little or no access to the internet without subjecting themselves to discrimination. The Commission 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>305</sup>

Even if a consumer can act to avoid discrimination, to require the consumer to do so is to require them to self-segregate, which is contrary to the fundamental tenet that “the doctrine of ‘separate but equal’ has no place” and is “inherently unequal.”<sup>306</sup> We have seen where it leads when one endorses the notion that discrimination is avoidable and it is the individual’s own fault when they fail to avoid it. The Supreme Court majority wrote in *Plessy v. Ferguson* that if “the enforced separation of the two races stamps the colored race with a badge of inferiority . . . it is not by reason of anything found in the act [requiring segregation], but solely because the colored race chooses to put that construction upon it.”<sup>307</sup> This is not an error to repeat.

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>308</sup> The “imposition of a barrier” creates “the inability to compete on equal footing.”<sup>309</sup> Thus, even if alternative services are available, even if they are equal, it is inherently unfair to require consumers to avoid the harm. For example, in *Missouri ex rel. Gaines v. Canada*, a Black resident was denied admission to an all-white law school.<sup>310</sup> The Supreme Court held that even though he could avoid the discrimination by attending law school in another state, this did not negate his injury.<sup>311</sup> Likewise, the Supreme Court held in *McLaurin v. Oklahoma State Regents for Higher Education* that segregation in a university was unlawful even when the segregated

---

<sup>304</sup> See *infra* § VI.C.

<sup>305</sup> FTC, *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>306</sup> *Brown*, 347 U.S. at 495.

<sup>307</sup> *Plessy v. Ferguson*, 163 U.S. 537, 551 (1896).

<sup>308</sup> See, e.g., *Heckler*, 465 U.S. at 740 (discrimination causes stigmatic harm).

<sup>309</sup> *Ne. Fla. Chapter of Ass’n Gen. Contractors of Am. v. City of Jacksonville, Fla.*, 508 U.S. 656, 666 (1993).

<sup>310</sup> *Missouri ex rel. Gaines v. Canada*, 305 U.S. 337 (1938).

<sup>311</sup> *Id.* at 349.

student used “the same classroom, library, and cafeteria as students of other races” without indication of “any disadvantage.”<sup>312</sup> And in *Henderson v. United States*, the Court held that dining car segregation was unlawful even though the railway offered alternative dinner service to an excluded Black patron at no extra charge.<sup>313</sup> These and myriad other civil rights cases stand for the fundamental proposition that an individual cannot reasonably avoid discrimination because the very act of avoidance itself causes a substantial injury.

### 3. Discrimination does not have countervailing benefits.

Discrimination does not have countervailing benefits that outweigh its harms.<sup>314</sup> Arguments defending discriminatory data practices fail for the same reasons that arguments defending segregation and other forms of brick-and-mortar discrimination failed. Thus, there is no right for a business to discriminate, and the Commission should reject any attempt to frame as a countervailing benefit corporate assertions of acting in a consumer’s best interests, lack of aggregate demand for services, or economic efficiency—parochially or globally. However, as discussed below, narrowly tailored exceptions should be made for affirmative action, diversity initiatives, and programs for self-testing to identify biases.

There is no right for a business to discriminate. In *Heart of Atlanta Motel*, which tested the constitutionality of Title II of the Civil Rights Act of 1964, the business specifically framed “the fundamental issue” as “whether or not Congress has the power to take away the personal liberty of an individual to run his business as he sees fit with respect to the selection and service of his customers” and contended that Black peoples’ loss of rights was “purely incidental.”<sup>315</sup> The petitioner analogized this “basic right to pursue his calling” as “a right just as fundamental to his life and liberty as such other high priority freedoms, to wit, freedom of speech and freedom of religion” and contended that an obligation to “furnish[] labor or services for certain individuals for whom he does not desire to work is obviously coercion if not outright punishment.”<sup>316</sup> The Supreme Court squarely

---

<sup>312</sup> *McLaurin v. Okla. State Regents for Higher Educ.*, 339 U.S. 637, 640–42 (1950).

<sup>313</sup> *See id.* at 818.

<sup>314</sup> *See Napleton Statement*, *supra* note 108, at 3; *Passport Auto. Grp. Statement*, *supra* note 108, at 2.

<sup>315</sup> Brief for Petitioner, *Heart of Atlanta Motel v. United States*, 379 U.S. 241, 1964 WL 81380, at \*32 (1964) (No. 515).

<sup>316</sup> *Id.* at \*57.

rejected these arguments and the claim that Title II violated the legal rights of businesses.<sup>317</sup>

Stopping discrimination is a “highest order” public good that not even other constitutional rights can surpass. When the government seeks to “eliminat[e] discrimination and assur[e] its citizens equal access to publicly available goods and services” that goal “plainly serves compelling state interests of the highest order.”<sup>318</sup> The Supreme Court has repeatedly confirmed that rights to free speech, free association, property, contract, and other liberties do not excuse discrimination. Measured against the value of eliminating inequity, any purported right to discriminate or value of discrimination receives little weight. The Supreme Court has rejected the idea that in “every setting in which individuals exercise some discrimination in choosing associates, their selective process of inclusion and exclusion is protected by the Constitution.”<sup>319</sup> There is no First Amendment associational right to discriminate in employment,<sup>320</sup> in who may attend a private school,<sup>321</sup> or who may join a labor union.<sup>322</sup> “Invidious private discrimination may be characterized as a form of exercising freedom of association protected by the First Amendment, but it has never been accorded affirmative constitutional protections.”<sup>323</sup> Even if an anti-discrimination law imposes some infringement on First Amendment rights, “the infringement is justified because it serves the State’s compelling interest in eliminating discrimination.”<sup>324</sup> Nor do platforms have a First Amendment right to structure content for the purpose of facilitating the discrimination of others. In *Pittsburgh Press Co. v. Pittsburgh Comm’n on Human Relations*, the Supreme Court held that an anti-discrimination law prohibiting

---

<sup>317</sup> *Heart of Atlanta Motel*, 379 U.S. at 260.

<sup>318</sup> *Roberts v. U.S. Jaycees*, 468 U.S. 609, 624 (1984).

<sup>319</sup> *N.Y. State Club Ass’n v. City of New York*, 487 U.S. 1, 13–14 (1988).

<sup>320</sup> *Hishon v. King & Spaulding*, 467 U.S. 69, 78 (1984); see also *Burwell v. Hobby Lobby Stores, Inc.*, 573 U.S. 682, 733 (2014) (“[T]he Government has a compelling interest in providing an equal opportunity to participate in the workforce without regard to race, and prohibitions on racial discrimination are precisely tailored to achieve that critical goal.”).

<sup>321</sup> *Runyon v. McCrary*, 427 U.S. 160 (1976); see also *Bob Jones Univ. v. United States*, 461 U.S. 574, 604 (1983) (“[T]he Government has a fundamental, overriding interest in eradicating racial discrimination in education.”).

<sup>322</sup> *Railway Mail Ass’n. v. Corsi*, 326 U.S. 88, 93–94 (1945).

<sup>323</sup> *Norwood v. Harrison*, 413 U.S. 455, 470 (1973).

<sup>324</sup> *Bd. of Dirs. of Rotary Int’l v. Rotary Club of Duarte*, 481 U.S. 537, 549 (1987).

newspapers from publishing job advertisements in sex-segregated columns did not violate the First Amendment.<sup>325</sup>

Discrimination cannot be countervailed by assertions of efficiency or paternalistic stereotyping that a firm is doing what they think is in a consumer's best interest. These types of rationales have long been rejected in civil rights case law. For example, in *Henderson*, the Supreme Court rejected the Southern Railway Company's defense of dining car segregation that "[t]he separation of the races is based upon considerations of the safety, comfort, and general satisfaction of travelers of both races."<sup>326</sup> Likewise in *Pittsburgh Press*, a newspaper defended sex-segregated classified ads on the grounds that the segregation was "for the convenience of its readers" as "most jobs generally appeal more to persons of one sex than the other."<sup>327</sup>

It is also well-established that discrimination does not become fair or "canceled out" if a firm is discriminating against everyone in different ways. In *Shelley v. Kraemer*, the Supreme Court rejected this argument when considering a law that discriminated against both white home sellers and Black home buyers, holding, "Equal protection of the laws is not achieved through indiscriminate imposition of inequalities."<sup>328</sup>

Appeal to the lack of aggregate demand for services is also not a countervailing factor. The Supreme Court rejected this argument in *Henderson*. "It is argued that the limited demand for dining-car facilities" by Black passengers "justifies the regulations. But it is no answer to the particular passenger who is denied service at an unoccupied place in the dining car that, on the average, persons like him are served."<sup>329</sup> Similarly in another railroad segregation case, *Mitchell v. United States*, the Court held that "the comparative volume of traffic cannot justify the denial of a fundamental right of equality of treatment."<sup>330</sup> "While the supply of particular facilities may be conditioned upon there being a reasonable demand therefor, if facilities are provided, substantial equality of treatment of persons

---

<sup>325</sup> *Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations*, 413 U.S. 376 (1973).

<sup>326</sup> Brief for Southern Railway Co., *Henderson v. United States*, 339 U.S. 816, 1949 WL 50331, at \*26 (1950) (No. 25).

<sup>327</sup> *Pittsburgh Press*, 413 U.S. at 381 n.7

<sup>328</sup> *Shelley v. Kraemer*, 334 U.S. 1, 22 (1948); see also *Bostock v. Clayton County, Ga.*, 140 S.Ct. 1731, 1741 (2020) ("Nor is it a defense for an employer to say it discriminates against both men and women because of sex . . . Instead of avoiding Title VII exposure, this employer doubles it.").

<sup>329</sup> *Henderson*, 339 U.S. at 825.

<sup>330</sup> *Mitchell v. United States*, 313 U.S. 80, 97 (1941).

traveling under like conditions cannot be refused.”<sup>331</sup> Notably, both *Henderson and Mitchell* were interpreting the unfairness provision of the Interstate Commerce Act, which is similar to the FTC Act.<sup>332</sup>

Appeals to economic efficiency also fail to demonstrate countervailing benefits. As a threshold matter, *even if* one assumes that discrimination is more efficient and profitable to the firm and its shareholders, that does not mean it is better for the public interest. The total utility to *society at large* must be considered, and that includes not just the individuals directly affected, but also their broader communities and even subsequent generations.<sup>333</sup> Compared to these monumental inequities, a few points on a firm’s balance sheet are nothing.

Indeed, there is extensive research documenting, in economic terms, discrimination’s harmful societal impact and the positive effects of increasing integration and diversity. For example, one recent study of changes in occupational distributions of people from 1960 to 2010 suggested that a significant number of women and Black men did not pursue occupations for which they were qualified.<sup>334</sup> The effect of reduction in barriers to employment could explain “between 20% and 40% of growth in the aggregate market output per person.”<sup>335</sup> Another study examined the effects of Jim Crow hate-related violence on innovation and estimated that it substantially reduced patents filed by Black Americans, suggesting that discrimination can reduce the quality of aggregate technological development and economic growth.<sup>336</sup> Citi Bank recently studied the effects of racial discrimination: “If racial gaps for Blacks had been closed 20 years ago, the U.S. GDP could have benefitted by an estimated \$16 trillion. If we close gaps today, the equivalent add to the U.S. economy over the next five years could be \$5 trillion of additional GDP, or an average add of 0.35 percentage points to U.S. GDP growth per year and 0.09 percentage points to global GDP growth per year.”<sup>337</sup> The consultancy McKinsey & Co. has

---

<sup>331</sup> *Id.*

<sup>332</sup> *See infra* § V.C.

<sup>333</sup> *See supra* §§ II & III.

<sup>334</sup> Chang-Tai Hsieh et al., *The Allocation of Talent and U.S. Economic Growth*, 87 *Econometrica* 1439 (Sept. 2019), <http://klenow.com/HHJK.pdf>.

<sup>335</sup> *Id.*

<sup>336</sup> Lisa D. Cook, *Violence and economic activity: evidence from African American patents, 1870-1940*, 19 *J. Econ. Growth* 221 (2014), [https://lisadcook.net/wp-content/uploads/2014/02/pats\\_paper17\\_1013\\_final\\_web.pdf](https://lisadcook.net/wp-content/uploads/2014/02/pats_paper17_1013_final_web.pdf).

<sup>337</sup> Citi GPS: Global Perspectives & Solutions, *Closing the Racial Inequality Gaps: The Economic Cost of Black Inequality in the U.S.* (Sept. 2020),

published a series of reports documenting the economic and competitive advantages of diversity and inclusion programs in the workplace.<sup>338</sup> “Companies in the top quartile for racial and ethnic diversity are 35 percent more likely to have financial returns above their respective national industry medians” and “Companies in the top quartile for gender diversity are 15 percent more likely.”<sup>339</sup> “The most diverse companies are now more likely than ever to outperform less diverse peers on profitability.”<sup>340</sup>

However, the Commission’s regulations should account for fair, non-predatory uses of protected characteristics for the narrowly tailored purpose of increasing opportunities for underrepresented and historically marginalized communities. For example, privacy legislation currently pending before Congress, the American Data Privacy and Protection Act, includes exceptions that allow the processing of personal data related to protected characteristics for the purposes of either (1) internal self-testing to prevent discrimination, or (2) to expand an applicant, candidate, or customer pool to promote diversity, equity, or inclusion.<sup>341</sup>

\* \* \*

In sum, discrimination causes substantial injury to consumers, is not reasonably avoidable, and—except in a few narrowly tailored circumstances—does not have countervailing benefits. Therefore, it is an unfair trade practice and the Commission has a statutory obligation to prevent firms from engaging in it.<sup>342</sup>

---

[https://ir.citi.com/NvIUklHPilz14Hwd3oxqZBLMn1\\_XPqo5FrxsZD0x6hhil84ZxaxEuJUW-mak51UHvYk75VKeHCMl%3D](https://ir.citi.com/NvIUklHPilz14Hwd3oxqZBLMn1_XPqo5FrxsZD0x6hhil84ZxaxEuJUW-mak51UHvYk75VKeHCMl%3D).

<sup>338</sup> Sundiatu Dixon-Fyle et al., *Diversity wins: How inclusion matters*, McKinsey & Co. (May 19, 2020), <https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-wins-how-inclusion-matters>; Dame Vivian Hunt et al., *Delivering through diversity*, McKinsey & Co. (Jan. 18, 2018), <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/delivering-through-diversity>; Dame Vivian Hunt et al., *Why diversity matters*, McKinsey (Jan. 1, 2015), <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/why-diversity-matters>.

<sup>339</sup> Hunt et al., *Why diversity matters*, *supra* note 338.

<sup>340</sup> Dixon-Fyle et al., *Diversity wins: How inclusion matters*, *supra* note 338.

<sup>341</sup> See American Data Privacy and Protection Act (“ADPPA”), H.R. 8152, 117th Cong. § 207(a)(2)(A) (2022). ADPPA has gone through several drafts and amendments. The most recent version reported out of markup in the House Energy and Commerce Committee on July 20, 2022 and is available here: <http://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-1178152rh.pdf>.

<sup>342</sup> 15 U.S.C. § 45(a)(1), (a)(2), (n).

## B. Discrimination, if undisclosed, is a deceptive trade practice

Discrimination—if it is not disclosed to the consumer—is also a deceptive trade practice. This is well established in the Commission’s precedents, which have held housing advertisements to be deceptive when they failed to disclose that the landlords refused to rent to Black tenants.<sup>343</sup> “An advertiser’s failure to disclose material facts in circumstances where the effect of nondisclosure is to deceive a substantial segment of the public is as much deception as if it were accomplished through affirmative misrepresentations. ‘To tell less than the whole truth is a well-known method of deception.’”<sup>344</sup>

Causing unjustified disparate impacts without disclosure, in particular, is a deceptive trade practice because it will not be obvious to an individual consumer that discrimination is occurring—a material omission.<sup>345</sup> This is particularly true of automated decision-making systems, other algorithms, and other commercial surveillance technologies that produce discriminatory results within a black box, especially if the firm designing or operating the technology touts the fairness or neutrality of the tool.<sup>346</sup> The Commission should promulgate rules under Section 5 of the FTC Act that companies have an obligation to disclose when they are discriminating either intentionally or by disparate impact.

The remedy for deception typically is disclosure.<sup>347</sup> “The Commission is the expert body to determine what remedy is necessary to eliminate the unfair or deceptive trade practices that have been disclosed. It has wide latitude for judgment and the courts will not interfere except where the remedy selected has no reasonable relation to the unlawful practices found to exist.”<sup>348</sup>

---

<sup>343</sup> See *In re E.G. Reinsch, Inc.*, 75 F.T.C. 210, 1969 WL 101036 (1969) (*Reinsch II*); *In re E.G. Reinsch, Inc.*, 74 F.T.C. 861, 1968 WL 94732 (1968) (*Reinsch I*); *In re First Buckingham Cmty., Inc.*, 73 F.T.C. 938, 1968 WL 94609 (1968).

<sup>344</sup> *First Buckingham*, 73 F.T.C. 938, 1968 WL 94609, at \*6 (quoting *P. Lorillard Co. v. Fed. Trade Comm’n*, 186 F.2d 52, 58 (4th Cir. 1950)).

<sup>345</sup> See *id.*

<sup>346</sup> See *infra* § VI.B.

<sup>347</sup> See, e.g., Enforcement Policy Statement on Deceptively Formatted Advertisements, 81 Fed. Reg. 22596, 22596 (Apr. 18, 2016) (“Any qualifying information necessary to prevent deception must be disclosed prominently and unambiguously to overcome any misleading impression created.”); *Warner-Lambert Co. v. Fed. Trade Comm’n*, 562 F.2d 749, 762 (D.C. Cir. 1977) (approving the Commission’s policy for requiring corrective advertisements).

<sup>348</sup> *Jacob Siegel Co. v. Fed. Trade Comm’n*, 327 U.S. 608, 612–13 (1946).

Disclosure would have profound consequences, even if it is not a complete remedy. First, it would illustrate the Commission’s role amid other government actors in combatting discrimination. Second, bringing transparency to the discrimination allows other federal agencies and state attorney generals with other legal authorities to bring them to bear on the discriminatory practice, as appropriate. Third, in cases of disparate impact, if the firm discloses that it is engaging in a practice causing an unjustified disparate impact *and continues the practice*, then it could be liable for not just disparate impact but disparate treatment, because it knows it is causing a discriminatory effect and continues anyway.<sup>349</sup> This in turn may trigger the application of other anti-discrimination laws that apply only to intentional discrimination.<sup>350</sup>

### **C. The FTC Act applies to both intentional discrimination and disparate impact.**

We respond to ANPR question 67, in which the Commission asks how it should handle intentional discrimination and discrimination by disparate impact.<sup>351</sup> The FTC Act encompasses both intentional discrimination and disparate impact.

Discrimination typically occurs in two forms: intentional discrimination and discrimination by disparate impact. Intentional discrimination is when a person intentionally or knowingly engages in disparate treatment of another person or class of persons on the basis of actual or perceived protected characteristics.<sup>352</sup> The “actual or perceived” qualifier is important—what matters is the motive of the perpetrator, not the actual traits of the

---

<sup>349</sup> See, e.g., *Columbus Bd. of Educ. v. Penick*, 443 U.S. 449, 464–65 (1979) (“[A]ctions having foreseeable and anticipated disparate impact are relevant evidence to prove the ultimate fact, forbidden purpose. . . . Adherence to a particular policy or practice, with full knowledge of the predictable effects of such adherence upon racial imbalance in a school system is one factor among many others which may be considered by a court in determining whether an inference of segregative intent should be drawn.” (cleaned up)); *N.C. State Conf. of NAACP v. McCrary*, 831 F.3d 204, 223–34 (4th Cir. 2016) (“A historical pattern of laws producing discriminatory results provides important context for determining whether the same decisionmaking body has also enacted a law with discriminatory purpose.” (citation omitted)).

<sup>350</sup> See, e.g., 42 U.S.C. §§ 1981, 1982, 2000a; Unruh Civil Rights Act, Cal. Civ. Code § 51.

<sup>351</sup> See ANPR, 87 Fed. Reg. at 51284.

<sup>352</sup> See, e.g., *Bostock*, 149 S.Ct. at 1740; *Columbus Bd. of Educ.*, 443 U.S. at 464–65 (1979).

victim. If the perpetrator mistakenly perceives someone to be a certain class and treats them adversely as a result, that still counts as intentional discrimination.<sup>353</sup>

Disparate impact involves discrimination that is unintentional—it occurs when a facially neutral action produces disproportionately adverse effects on a protected class.<sup>354</sup> Even when a statute prohibits discriminatory disparate impacts—such as the Fair Housing Act or Title VII—not all practices that produce disparate impacts are inherently unlawful.

The Supreme Court has established a three-part test to determine whether a practice is unjustified: First, the petitioner must establish that a facially neutral practice creates a disparate impact on the basis of a protected characteristic. Second, the respondent has the burden to show that they have a legitimate nondiscriminatory rationale justifying the practice. Then, if such rationale is established, the burden shifts back to the petitioner to show either that the proffered rationale is a pretext for discrimination or that such rationale could be met by a less discriminatory alternative.<sup>355</sup>

The prohibition of unfair and deceptive trade practices under Section 5 of the FTC Act encompasses disparate impact claims. Statutes “must be construed to encompass disparate-impact claims when their text refers to the consequences of actions and not just the mindset of actors, and where that interpretation is consistent with statutory purpose.”<sup>356</sup> The FTC Act declares unlawful “unfair or deceptive acts or practices in or affecting commerce”<sup>357</sup> and “empower[s] and direct[s]” the Commission “to prevent persons . . . from using . . . unfair or deceptive acts or practices in or affecting commerce.”<sup>358</sup> The Act further explains that to declare an act or practice to be unfair, the act or practice must “caus[e] or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”<sup>359</sup> This is known as the Unfairness Doctrine.

---

<sup>353</sup> See, e.g., *Griffin v. Breckenridge*, 403 U.S. 88, 90 (1971) (conspiracy to deprive civil rights occurred where perpetrators mistakenly thought the white driver of a car carrying Black passengers was a civil rights activist, which was a protected class).

<sup>354</sup> *Texas Dep’t of Hous. & Cmty. Affs. v. Inclusive Cmty. Project, Inc.*, 576 U.S. 519, 524 (2015).

<sup>355</sup> See *id.* at 533.

<sup>356</sup> *Id.*

<sup>357</sup> 15 U.S.C. § 45(a)(1).

<sup>358</sup> *Id.* § 45(a)(2).

<sup>359</sup> *Id.* § 45(n).

The Unfairness Doctrine encompasses disparate impact because it “refers to the consequences of actions” and makes no mention of “the mindset of actors.”<sup>360</sup> Section 5 focuses on how a practice “causes or is likely to cause” harm, not the intent of the actor.<sup>361</sup> This is similar structurally to the phrase at issue in *Inclusive Communities Project*, “otherwise make unavailable,”<sup>362</sup> because both are focused on effects: whether an action “causes” or “makes” something happen. In that case, the Supreme Court held that the Fair Housing Act did encompass disparate impact because “Congress’ use of the phrase ‘otherwise make unavailable’ refers to the consequences of an action rather than the actor’s intent. This results-oriented language counsels in favor of recognizing disparate-impact liability.”<sup>363</sup> The language in the FTC Act functions the same way.

Encompassing disparate impact within the Unfairness Doctrine is also consistent with the statutory purpose of the FTC Act, which commands the FTC to prevent persons from engaging in unfair trade practices regardless of motive.<sup>364</sup> The Commission should conclude that the Unfairness Doctrine applies to disparate impact scenarios and use the traditional three-part test that is well established in case law.

#### **D. The FTC should recognize a diverse array of protected characteristics.**

We respond now to ANPR questions 65, 67, and 68 in which the Commission asks what characteristics it should recognize for protection against discrimination.<sup>365</sup> The Commission should look to the categories that have been recognized for protection under other anti-discrimination laws at both the state and federal level.<sup>366</sup> Because the scope of Section 5 of the FTC Act is broad and remedial—a mandate to stop *all* unfair or deceptive

---

<sup>360</sup> *Inclusive Cmty. Project*, 576 U.S. at 533.

<sup>361</sup> 15 U.S.C. 45(n).

<sup>362</sup> *Inclusive Cmty. Project*, 576 U.S. at 533–34.

<sup>363</sup> *Id.* at 534.

<sup>364</sup> See 15 U.S.C. § 45(a)(2).

<sup>365</sup> ANPR, 87 Fed. Reg. at 51284.

<sup>366</sup> See David Brody & Sean Bickford, *Discriminatory Denial of Service: Applying State Public Accommodations Laws to Online Commerce*, Lawyers’ Committee (Jan. 2020), <https://lawyerscommittee.org/wp-content/uploads/2019/12/Online-Public-Accommodations-Report.pdf>.

trade practices in commerce—the Commission should generously construe the scope of the characteristics being protected to effectuate this remedial purpose.<sup>367</sup>

The Commission should recognize the following protected characteristics: race, color, ethnicity, national origin, caste, religion, sex, sexual orientation, gender identity or expression, disability, family responsibilities or familial status, pregnancy or pregnancy-related medical condition (including breastfeeding), place of residence, immigration status, housing status, personal appearance, genetic information, age, and status as a victim or family member (excluding perpetrator) of a victim of domestic violence, a sexual offense, stalking, or harassment.

Several of these categories are quite common to many anti-discrimination laws of all types, such as race, color, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, and disability.<sup>368</sup> Notably, members of these protected classes are generally protected by public accommodations laws that apply to all forms of commerce.<sup>369</sup> Each of the others is recognized in at least some anti-discrimination laws at the state or federal level, some in public accommodations laws and some in sectoral laws. Some of these characteristics may be protected in certain sectors and not others. For example, the Age Discrimination in Employment Act makes it illegal to discriminate on the basis of age in employment,<sup>370</sup> but age typically is not a protected characteristic in some other settings such as education, housing, or healthcare.

---

<sup>367</sup> See, e.g., *City of Memphis v. Greene*, 451 U.S. 100, 121 (1981) (Civil Rights Act of 1866 is “broadly construed” to “effectuate the remedial purposes of the statute”); *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967) (interpreting Securities Exchange Act and stating “we are guided by the familiar canon of statutory construction that remedial legislation should be construed broadly to effectuate its purposes.”);

<sup>368</sup> See, e.g., Cal. Civ. Code § 51; Colo. Rev. Stat. Ann. § 24-34-601; Conn. Gen. Stat. Ann. § 46a-60; Del. Code § 450; D.C. Code § 2-1402.31; Haw. Rev. Stat. §489-3; 75 Ill. Comp. Stat. Ann. § 5/1-102–103; Iowa Code § 216.7; Me. Rev. Stat. tit. 5, § 4591; Md. Code Ann., State Gov’t § 20-304; Mass. Gen. Laws Ann. ch. 272, § 98; Minn. Stat. Ann. §§ 363A.11; Nev. Rev. Stat. Ann. § 651.070; N.J. Stat. Ann. § 10:5-12; N.M. Stat. Ann. § 28-1-7; N.Y. Exec. Law § 29; Or. Rev. Stat. Ann. § 659A.403; § 174.100; 43 Pa. Stat. Ann. § 953; 11 R.I. Gen. Laws Ann. § 11-24-2; Vt. Stat. Ann. tit. 9, § 4502; Wash. Rev. Code Ann. § 49.60.215; Wis. Stat. Ann. § 106.52.

<sup>369</sup> See 42 U.S.C. § 2000a; *id.* § 12182; Brody & Bickford, *supra* note 366.

<sup>370</sup> 29 U.S.C. § 623.

## **V. The FTC has authority and responsibility to address discrimination and commercial surveillance practices.**

The history of the Commission, as well as the role its sister commissions have played in combatting racial discrimination, counsels in favor of the Commission taking action against commercial surveillance. In this section we respond to the Commission's questions 62, 69, 70, 71, and 72 about the legal authorities available to it, its relationship to other federal agencies, and the role it can and should play in addressing discrimination globally and in specific sectors.<sup>371</sup>

### **A. There are gaps in federal civil rights laws that the FTC can address.**

Major gaps in federal civil rights and privacy laws support the need for the Commission to engage in regulation to prevent data-driven discrimination and protect data privacy. At the same time, overlaps in various civil rights regimes have never been a serious obstacle to concurrent enforcement; companies routinely comply with parallel regimes under federal law and between federal and state law. As discussed below, the Commission's longstanding precedents hold that it can enforce Section 5 against race discrimination in parallel to other federal laws.

If existing civil rights laws and enforcement resources were adequate to protect against data-driven discrimination, we would not be seeing many of these problems in the first place.

Currently, there is no comprehensive federal privacy law. Existing anti-discrimination laws have many gaps and limitations as well. Some, such as Title II of the Civil Rights Act of 1964, exclude retail stores or have unresolved questions about how they apply to online businesses.<sup>372</sup> Others, such as the Fair Housing Act and Title VII, apply to specific sectors like housing and employment, respectively, but may not cover new types of online services used to match individuals to these opportunities. To give a few examples, under current federal civil rights statutes it would be legal for an online business to charge higher prices to women or to refuse to sell products to Christians.<sup>373</sup> A service provider could

---

<sup>371</sup> ANPR, 87 Fed. Reg. at 51284.

<sup>372</sup> See 42 U.S.C. § 2000a.

<sup>373</sup> See *id.* § 1981 (prohibiting discrimination in commerce solely on the basis of race and national origin); 42 U.S.C. § 2000a (prohibiting discrimination in public accommodations, but not retail stores, and omitting sex as a protected characteristic); *Shaare Tefila Congregation v. Cobb*, 481 U.S. 615 (1987) (Section 1981 applies to discrimination against Jews because they were considered a race in 1866 when the statute was enacted).

use discriminatory algorithms to look for workers to target for recruitment so long as the provider does not meet the definition of an “employment agency” under Title VII.<sup>374</sup>

Some federal civil rights laws are not comprehensive in the classes they protect. Sections 1981 and 1982 of the Civil Rights Act of 1866, and Title VI of the Civil Rights Act of 1964, only apply to race and national origin.<sup>375</sup> Title II additionally applies to religion.<sup>376</sup> But these core statutes do not apply to sex.<sup>377</sup> The scope of classes protected by Section 1985,<sup>378</sup> which prohibits conspiracies against civil rights and has been used to combat commercial discrimination,<sup>379</sup> is unsettled.<sup>380</sup> And in general, federal civil rights laws may not always cover discrimination against LGBTQ+ individuals, although the Supreme Court has held that discrimination “because of sex” includes discrimination on the basis of sexual orientation or gender identity.<sup>381</sup>

Many existing federal civil rights statutes also apply only to intentional discrimination and do not apply to disparate impact. Sections 1981 and 1982, as well as Title II, apply only to intentional discrimination.<sup>382</sup> The Fair Housing Act, Title VII, and the Equal Credit Opportunity Act (“ECOA”), among other statutes, apply to disparate impact.<sup>383</sup> The

---

<sup>374</sup> See generally Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn (2018), <https://www.upturn.org/reports/2018/hiring-algorithms/>.

<sup>375</sup> 42 U.S.C. §§ 1981, 1982, 2000d.

<sup>376</sup> *Id.* § 2000a.

<sup>377</sup> Title IX extends anti-discrimination protections similar to Title VI to sex discrimination, but only in the context of education. 20 U.S.C. § 1681.

<sup>378</sup> 42 U.S.C. § 1985.

<sup>379</sup> See, e.g., *Washington v. Duty Free Shoppers*, 696 F. Supp. 1323 (N.D. Cal. 1988).

<sup>380</sup> See, e.g., *Bray v. Alexandria Women’s Health Clinic*, 506 U.S. 263 (1993) (scope of protected classes undecided); *United Bhd. of Carpenters & Joiners of Am., Loc. 610, AFL-CIO v. Scott*, 463 U.S. 825 (1983) (1985(3) scope is undecided, but it does not apply to conspiracies against union organizers).

<sup>381</sup> See *Bostock*, 140 S.Ct. 1731.

<sup>382</sup> *Gen. Bldg. Contractors Ass’n v. Pennsylvania*, 458 U.S. 375, 391 (1982) (Section 1981); *Daniels v. Dillard’s, Inc.*, 373 F.3d 885, 888 n.4 (8th Cir. 2004) (Section 1982); *Joseph v. Metro. Museum of Art*, No. 1:15-CV-9358-GHW, 2016 WL 3351103, at \*2 (S.D.N.Y. June 15, 2016), *aff’d*, 684 F. App’x 16 (2d Cir. 2017) (Title II).

<sup>383</sup> See *Texas Dep’t of Hous. & Cmty. Affs. v. Inclusive Communities Project, Inc.*, 576 U.S. 519, 545 (2015) (Fair Housing Act); *Griggs v. Duke Power Co.*, 401 U.S. 424, 431 (1971) (Title VII); Michael Aleo & Pablo Svirsky, *Foreclosure Fallout: The Banking*

federal government can administratively enforce Title VI to address disparate impacts, but private litigants can only bring intentional discrimination claims.

There are also sectors that lack comprehensive sector-specific civil rights laws akin to the Fair Housing Act or ECOA. For example, Title IX addresses sex discrimination in educational opportunities receiving federal funding,<sup>384</sup> but there is no comprehensive anti-discrimination statute specific to education. Likewise, while the Fair Housing Act, ECOA, and regulations from the Department of Health and Human Services can apply to some forms of insurance discrimination, there is no general civil rights law specific to insurance. It is also unclear whether existing laws will apply at all to discrimination in many new online-only economies related to online gaming, influencers, streamers, and other creators. The scope of ECOA's application to novel online financial products is also unclear.

While there are gaps in federal civil rights protections, there also are overlaps. Although some laws are sectoral, it is common for laws prohibiting discrimination to apply to the entire economy—such as Section 1981, Section 1985,<sup>385</sup> and the public accommodations laws of 41 states and the District of Columbia.<sup>386</sup> Other laws cover wide ranges of conduct. For example, Section 1982 applies only to property rights, but it addresses

---

*Industry's Attack on Disparate Impact Race Discrimination Claims Under the Fair Housing Act and the Equal Credit Opportunity Act*, 18 B.U. Pub. Int. L.J. 1, 62 n.467 (2008) (ECOA) (collecting cases).

<sup>384</sup> See 20 U.S.C. § 1681.

<sup>385</sup> See, e.g., *Vietnamese Fishermen's Ass'n v. Knights of the Ku Klux Klan*, 518 F.Supp. 993 (S.D. Tex. 1981) (Klansmen violated Section 1985 by intimidating Vietnamese fishermen seeking to engage in commercial shrimping).

<sup>386</sup> See Alaska Stat. Ann. § 18.80.300; Ariz. Rev. Stat. Ann. § 41-1441; Ark. Code Ann. § 16-123-102; Calif. Civ. Code § 51; Colo. Rev. Stat. Ann. § 24-34-601; Conn. Gen. Stat. Ann. § 46a-63; 6 Del. Code § 4502; D.C. Code § 2-1401.02(24); Haw. Rev. Stat. An.. § 489-2; Idaho Code An.. § 67-5902; Ind. Code Ann. § 22-9-1-3; Iowa Code § 216.2; Kan. Stat. Ann. § 44-1002; Ky. Rev. Stat. § 344.130; La. Stat. Ann. § 51:2232; Me. Rev. Stat. tit. 5, §4553; Md. Code Ann., State Gov't § 20-301; Mass. Gen. Laws Ann. Ch. 272, § 92A; Mich. Comp. Laws Ann. § 37.1301; Minn. Stat. Ann. § 363A.03; Mo. Ann. Stat. § 213.010; Mont. Code Ann. § 49-2-101; Neb. Rev. Stat. Ann. § 20-133; Nev. Rev. Stat. Ann. § 651.050; N.H. Rev. Stat. Ann. §354-A:2; N.J. Stat. Ann. § 10:5-5; N.M. Stat. Ann. § 28-1-2; N.Y. Exec. Law § 292; N.D. Cent. Code Ann. § 14-02.4-02; Ohio Rev. Code Ann. § 4112.01(A)(9); Okla. Stat. Ann. Tit. 25, § 1401; Or. Rev. Stat. Ann. § 659A.400; 43 Pa. Stat. Ann. § 954; 11 R.I. Gen. Laws Ann. § 11-24-3; S.D. Codified Laws § 20-13-1; Tenn. Code Ann. § 4-21-102; Utah Code Ann. § 13-7-3; Vt. Stat. Ann. Tit. 9, § 4501; Wash. Rev. Code Ann. § 49.60.040; W. Va. Code Ann. § 5-11-3; Wis. Stat. Ann. § 106.52; Wyo. Stat. Ann. § 6-9-101.

housing discrimination, hate crimes against property, and more.<sup>387</sup> Moreover, as the law has evolved to better cover new discriminatory practices and expand protections to additional classes of people, new civil rights laws often overlap with older civil rights laws.

It is neither uncommon nor problematic for multiple statutes or multiple agencies to address the same subject matter. Nor is it a problem to administer overlapping regimes; courts have been doing it for decades.<sup>388</sup> For example, at least five statutory regimes apply directly to fair housing, including the Fair Housing Act, Section 1981, Section 1982, ECOA, and the Home Mortgage Disclosure Act. At least six regimes apply directly to equal opportunity in employment, including Title VII, Section 1981, Title VI, the Age Discrimination in Employment Act, the Americans with Disabilities Act, and the Equal Pay Act of 1963. The Voting Rights Act, the National Voter Registration Act, Section 1985, and federal criminal voter suppression laws all apply to voting rights. Public accommodations are protected by at least four regimes, including Section 1981, Title II, the Americans with Disabilities Act, and federal criminal public accommodations laws. Various statutory and regulatory regimes apply to financial discrimination, including ECOA and Section 1981. Several different federal regimes apply to hate crimes as well, including Section 1981, Section 1982, Section 1985, the Freedom of Access to Clinic Entrances Act, the Violence Against Women Act, and federal criminal hate crimes laws. And, of course, most states have their own civil rights laws that, in some cases, go above and beyond federal law—but still have major shortcomings as well.<sup>389</sup>

As a result of gaps in federal law, individuals currently have little recourse against discriminatory algorithms and AI models used in commercial surveillance that reinforce the structural racism and systemic bias that pervade our society. Tech companies can misuse personal data, intentionally or unintentionally, to harm communities of color through deception, discrimination, exploitation, and perpetuation of redlining.<sup>390</sup> Without additional protections, it may be possible for online businesses to deny service on the basis of race or ethnicity, provide subpar products based on gender or sexual orientation,

---

<sup>387</sup> See, e.g., *Shaare Tefila Congregation*, 481 U.S. 615 (anti-Semitic vandalism of a synagogue could violate Section 1982).

<sup>388</sup> See, e.g., *Alfred H. Mayer Co.*, 392 U.S. at 416–17 (1968) (holding that the enactment of the Fair Housing Act “had no effect” on the older anti-discrimination statute, 42 U.S.C. § 1982, and instead “underscored the vast differences between . . . a general statute . . . and . . . a detailed housing law.”).

<sup>389</sup> See Brody & Bickford, *supra* note 366. Since the publication of this report, Nevada and the District of Columbia have amended their laws to apply to online public accommodations.

<sup>390</sup> See *supra* § III.

charge higher rates based on religion, or ignore the accessibility needs of persons with disabilities.<sup>391</sup>

**B. The FTC can address gaps with its authority to regulate unfair and deceptive practices. It has done this before.**

The Commission can and should fill the gaps. Indeed, the Commission itself has extensive experience sharing concurrent jurisdiction with other agencies. It works on ECOA with the Consumer Financial Protection Bureau, on antitrust with the Department of Justice, and on robocalls with the Federal Communications Commission. The Commission also has experience, *and precedent*, applying the FTC Act to discriminatory behaviors even when other agencies have concurrent jurisdiction.

In 1967 and 1968, in *In re E.G. Reinsch, Inc.*,<sup>392</sup> and *In re First Buckingham Cmty, Inc.*,<sup>393</sup> the Commission addressed race discrimination in housing advertisements. These cases were initiated in 1967, just prior to the passage of the Fair Housing Act as part of the Civil Rights Act of 1968. The Commission held it was a Section 5 violation for a housing provider to falsely represent in advertisements that apartments were available to the general public when in fact the landlords refused to consider Black applicants.<sup>394</sup> Respondents argued that recent passage of the Fair Housing Act rendered moot the Commission's enforcement of Section 5 against housing discrimination; the Commission disagreed. Holding that the advertisements were deceptive in violation of Section 5, the Commission reasoned in *First Buckingham*,

It is also clear that the enactment of the Civil Rights Act of 1968 does not render lawful any acts or practices which would otherwise be deemed unlawful under the Federal Trade Commission Act. Neither in its terms nor its legislative history does the Civil Rights Act disclose an intent by Congress to repeal or modify, in whole or in part, expressly or by implication, directly or indirectly, any provision of the Federal Trade Commission Act. Congress surely could not have intended, in passing the Civil Rights Act, to grant anyone a license to engage in false and misleading advertising that violates the Federal Trade Commission Act. Thus, if the facts presented

---

<sup>391</sup> See *id.*

<sup>392</sup> *Reinsch II*, 75 F.T.C. 210, 1969 WL 101036; *Reinsch I*, 74 F.T.C. 861, 1968 WL 94732.

<sup>393</sup> *First Buckingham*, 73 F.T.C. 938, 1968 WL 94609.

<sup>394</sup> See *Reinsch I*, 74 F.T.C. 861, 1968 WL 94732, at \*2; *First Buckingham*, 73 F.T.C. 938, 1968 WL 94609, at \*2–3, 6.

before the hearing examiner showed a violation of the Federal Trade Commission Act, it would be immaterial that they might also show a violation of the Civil Rights Act of 1968. Conduct that violates one federal statute does not become immune because it also violates another statute.<sup>395</sup>

The defendants in these cases pledged to the Commission that they were changing their policies to conform to newly enacted fair housing requirements, and the Commission dropped its complaints. But in both cases the Commission warned, “[A]n order to cease and desist may not now [be] necessary. . . . If it should appear in the [future] however, that we are mistaken in this regard, the matter can always be reopened.”<sup>396</sup> These precedents stand for two propositions: (1) The FTC Act can and should be used to combat race discrimination when it occurs through an unfair or deceptive practice; and (2) the Commission can exercise its anti-discrimination authority concurrently to other civil rights regimes.

Other Commission precedents, guidance, and policy statements counsel in favor of combatting discrimination as an unfair and deceptive trade practice. In 2005, in *In re BJ’s Wholesale Club*, the Commission established that corporate data handling practices that allow malicious misuse of personal data are unfair trade practices.<sup>397</sup> In 2011, in *FTC v. Frostwire LLC*, the Commission asserted that invasive data collection practices were unfair in part because they “reduce [consumers] ability to control the dissemination of personal or proprietary information” increasing the risk of harm.<sup>398</sup> The Commission’s 2012 privacy report noted the risk that privacy-invasive advertising practices involving

---

<sup>395</sup> *First Buckingham*, 73 F.T.C. 938, 1968 WL 94609, at \*7.

<sup>396</sup> *Reinsch I*, 74 F.T.C. 861, 1968 WL 94732, at \*3; accord *First Buckingham*, 73 F.T.C. 938, 1968 WL 94609, at \*7.

<sup>397</sup> See Complaint, *In re BJ’s Wholesale Club, Inc.*, FTC File No. 042 3160 (Sept. 23, 2005), <https://www.ftc.gov/legal-library/browse/cases-proceedings/042-3160-bjs-wholesale-club-inc-matter>; see also Complaint at 7–9, *United States v. Choicepoint*, No. 06-cv-0198 (N.D. Ga. Jan. 30, 2006), ECF No. 1 (FTC alleges inadequate data security was an unfair trade practice and enabled downstream illegal uses of consumer data).

<sup>398</sup> See Complaint ¶ 31, *FTC v. Frostwire LLC*, No. 11-cv-23643 (S.D. Fla. Oct. 7, 2011), ECF No. 1, <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf>; see also Stipulated Final Order for Permanent Injunction at 1, *FTC v. Frostwire LLC*, No. 11-cv-23543 (S.D. Fla. Oct. 12, 2011), ECF No. 5, <https://www.ftc.gov/legal-library/browse/cases-proceedings/112-3041-frostwire-llc-angel-leon> (finding complaint stated cognizable claims under § 5 of the FTC Act).

sensitive data “could lead to embarrassment, discrimination, or other harms.”<sup>399</sup> In a report on data brokers in 2014, the Commission warned that data brokers “take reasonable precautions to ensure that downstream users of their data do not use it for eligibility determinations or for unlawful discriminatory purposes.”<sup>400</sup>

In 2016, the Commission considered the risks of discrimination in the “big data” ecosystem, stating that under the FTC Act, “at a minimum, companies must not sell their big data analytics products to customers if they know or have reason to know that those customers will use the products for fraudulent or discriminatory purposes.”<sup>401</sup> This statement contains within it the implication that it would be a violation for the company itself to undertake such actions as well. The Commission continued, “the test will be whether the company is offering or using big data analytics in a deceptive or unfair way.”<sup>402</sup> The Commission also observed that “it is important to consider the digital divide and other issues of underrepresentation and overrepresentation in data inputs before launching a product or service in order to avoid skewed and potentially unfair ramifications.”<sup>403</sup> In 2021, the Commission issued guidance observing that Section 5 prohibits the sale or use of racially biased algorithms. “[L]et’s say the model pinpoints those consumers by considering race, color, religion, and sex—and the result is digital redlining[.] . . . If your model causes more harm than good . . . the FTC can challenge the use of that model as unfair.”<sup>404</sup>

More recently, the Commission has driven home in its enforcement actions the argument that discrimination is unfair. In *FTC v. Liberty Chevrolet, Inc.* (“*Bronx Honda*”) in 2020, the Commission brought claims alleging race discrimination in vehicle financing

---

<sup>399</sup> FTC, *Protecting Consumer Privacy in an Era of Rapid Change* 47 (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

<sup>400</sup> FTC, *Data Brokers: A Call for Transparency and Accountability* 55–56 (2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

<sup>401</sup> FTC, *Big Data: A Tool for Inclusion or Exclusion?*, *supra* note 301, at iv, 23.

<sup>402</sup> *Id.*

<sup>403</sup> *Id.* at 28.

<sup>404</sup> Elisa Jillson, *Aiming for truth, fairness, and equity in your company’s use of AI*, FTC (Apr. 19, 2021), <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

by an auto dealer.<sup>405</sup> Former Commissioner Rohit Chopra observed that “[u]sing disparate impact analysis and other tools, the Commission can use its unfairness authority to attack harmful discrimination in other sectors of the economy” than covered by existing laws.<sup>406</sup> Commissioner Rebecca Slaughter agreed that “discriminatory pricing practices” are a Section 5 violation and rulemaking is necessary.<sup>407</sup>

In April 2022, the Commission brought and settled a complaint against another auto dealer engaging in discrimination. In the *Napleton Auto* case, dealers were adding charges and raising interest rates for Black auto buyers that they did not impose on white buyers.<sup>408</sup> The FTC alleged that tacking on charges without consumers’ consent was an unfair practice.<sup>409</sup> Where those add-on charges were applied on the basis of race, without disclosure to the consumers, the fact pattern echoes the *First Buckingham* and *E.G. Rein-sch* anti-discrimination cases from the 1960s—both then and now the defendant businesses treated customers differently on the basis of race without disclosing that fact.

Along these lines, Chair Khan and Commissioner Slaughter stated that the discrimination at issue here is an unfair trade practice in violation of the FTC Act.<sup>410</sup> They observed that (1) “discrimination based on protected status is a substantial injury to consumers” including higher costs to Black buyers; (2) “injuries stemming from disparate treatment or impact are unavoidable because affected consumers cannot change their status or otherwise influence the unfair practices;” and (3) “injuries stemming from disparate treatment or impact are not outweighed by countervailing benefits to consumers or

---

<sup>405</sup> See Complaint, *FTC v. Liberty Chevrolet, Inc.*, No. 20-cv-03945 (S.D.N.Y. May 21, 2020), ECF No. 1, [https://www.ftc.gov/system/files/documents/cases/bronx\\_honda\\_complaint\\_0.pdf](https://www.ftc.gov/system/files/documents/cases/bronx_honda_complaint_0.pdf).

<sup>406</sup> Statement of Commissioner Rohit Chopra, *In re Liberty Chevrolet, Inc. d/b/a Bronx Honda*, FTC File No. 162 3238, at 2 (May 27, 2020), [https://www.ftc.gov/system/files/documents/public\\_statements/1576002/bronx\\_honda\\_final\\_rchopra\\_bronx\\_honda\\_statement.pdf](https://www.ftc.gov/system/files/documents/public_statements/1576002/bronx_honda_final_rchopra_bronx_honda_statement.pdf).

<sup>407</sup> Statement of Commissioner Rebecca Kelly Slaughter, *In re Liberty Chevrolet, Inc. d/b/a Bronx Honda*, FTC File No. 162 3238, at 4–5 (May 27, 2020), [https://www.ftc.gov/system/files/documents/public\\_statements/1576006/bronx\\_honda\\_2020-5-27\\_bx\\_honda\\_rks\\_concurrence\\_for\\_publication.pdf](https://www.ftc.gov/system/files/documents/public_statements/1576006/bronx_honda_2020-5-27_bx_honda_rks_concurrence_for_publication.pdf).

<sup>408</sup> See Complaint, *FTC v. N. Am. Auto. Servs., Inc.*, No. 22-cv-1690 (N.D. Ill. Mar. 31, 2022), ECF No. 1 [https://www.ftc.gov/system/files/ftc\\_gov/pdf/1%20-%20Joint%20Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/1%20-%20Joint%20Complaint.pdf) (“*Napleton Auto*”).

<sup>409</sup> *Id.* ¶¶ 76–78.

<sup>410</sup> *Napleton Statement*, *supra* note 108, at 3–4.

competition” in part because “[a]ny purported benefit that can be achieved without engaging in the conduct causing substantial injury is not countervailing.”<sup>411</sup>

In *FTC v. Passport Automotive Group*, the Commission adopted and put into practice Chair Kahn and Commissioner Slaughter’s position in the *Napleton Statement*.<sup>412</sup> The FTC alleged that Passport imposed higher borrowing costs on Black and non-white Latino consumers than on similarly situated non-Latino white customers and charged Passport with unfair discrimination in violation of Section 5.<sup>413</sup> The Settlement Order with Passport accordingly includes provisions against unlawful discrimination on the basis of race, color, religion, national origin, sex or marital status, or age.<sup>414</sup> As stated in the accompanying joint statement of Chair Kahn, Commissioner Slaughter, and Commissioner Bedoya, the discrimination charge was “a straightforward application of Section 5”:

Black and Latino consumers suffered substantial economic injury in the form of higher fees for the same products and services. These consumers could not reasonably avoid this injury, because they typically had no way of knowing they were being charged more than their White counterparts. And Passport’s pricing practices did not yield countervailing benefits.<sup>415</sup>

The Commission likewise is asserting unfairness claims directly in *FTC v. Kochava*.<sup>416</sup> In *Kochava*, the Commission alleges that defendants acquired and sold precise geolocation data of consumers in a manner that allowed the identification of individuals and the tracking of activities related to “medical care, reproductive health, religious

---

<sup>411</sup> *Id.*

<sup>412</sup> See Complaint ¶¶ 59–61, *FTC v. Passport Auto. Grp.*, No. 8:22-cv-02670-GLS (D. Md. Oct. 18, 2022), ECF No. 1, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/Complaint%20Passport%20Auto%20Group%2C%20Inc.%2C%20et%20al..pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint%20Passport%20Auto%20Group%2C%20Inc.%2C%20et%20al..pdf); Settlement Order for Permanent Injunction, Monetary Judgment, and Other Relief at 6–7, *FTC v. Passport Auto. Grp.*, No. 8:22-cv-02670-GLS (D. Md. Oct. 18, 2022), ECF No. 2-1, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/Order%20As%20Filed.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/Order%20As%20Filed.pdf); *Passport Auto. Grp. Statement*, *supra* note 108, at 2.

<sup>413</sup> Complaint ¶¶ 23–36, 59–61, *Passport Auto. Grp.*, No. 8:22-cv-02670-GLS.

<sup>414</sup> Settlement Order for Permanent Injunction, Monetary Judgment, and Other Relief at 6–7, *Passport Auto. Grp.*, No. 8:22-cv-02670-GLS.

<sup>415</sup> *Passport Auto. Grp. Statement*, *supra* note 108, at 1–2.

<sup>416</sup> See Complaint, *FTC v. Kochava, Inc.*, No. 22-cv-377 (D. Idaho Aug. 29, 2022), ECF No. 1, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/1.%20Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf).

worship, mental health, temporary shelters . . . and addiction recovery.”<sup>417</sup> Kochava’s practices are unfair and violate Section 5, the Commission argues, in part because the data “injures or is likely to injure consumers through exposure to stigma, discrimination, physical violence, emotional distress, and other harms.”<sup>418</sup>

It is true that the Commission has scarcely used its Section 5 authority to combat discrimination until recently. That lack of will should not be mistaken for a lack of authority. As the Supreme Court held, over 100 years after the passage of the Civil Rights Act of 1866, “The fact that the statute lay partially dormant for many years cannot be held to diminish its force today.”<sup>419</sup> The time to act is now, before modern commercial surveillance technologies become as entrenched as Jim Crow and cause intergenerational inequities.

**C. The FTC should consider how similar provisions of the Interstate Commerce Act were used to advance desegregation.**

When the Commission is considering what constitute “unfair or deceptive acts or practices in or affecting commerce,”<sup>420</sup> it should consider how a similar unfairness provision in the Interstate Commerce Act played a pivotal role in the dismantling of segregation in places of public accommodation. Indeed, President Franklin D. Roosevelt noted the similarity of the FTC’s role in preventing unfair trade practices to that of its predecessor commissions when he laid the FTC building’s cornerstone: “Most of the great federal commissions that have been set up . . . were constituted with the belief that an ounce of prevention was worth a pound of cure. And the Federal Trade Commission was no exception to that sound legislative intent. Prevention of unfair business practices is generally better than punishment administered after the fact of infringement.”<sup>421</sup> Just as the Interstate Commerce Act was used to challenge segregation, so too should the FTC Act.

---

<sup>417</sup> *Id.* ¶ 1.

<sup>418</sup> *Id.* ¶ 29.

<sup>419</sup> *Alfred H. Mayer Co.*, 392 U.S. at 437.

<sup>420</sup> 15 U.S.C. § 45(a).

<sup>421</sup> President Franklin D. Roosevelt, Address at the Cornerstone Laying Ceremonies for the New Federal Trade Commission Building (July 12, 1937), <https://www.ftc.gov/sites/default/files/attachments/federal-trade-commission-history/1937-fdr-speech.mp3>.

The FTC was modeled on the Interstate Commerce Commission (ICC).<sup>422</sup> That sister commission played a significant role, first as an obstacle and belatedly an ally, in the fight for racial integration in the years before and after *Brown v. Board of Education*, specifically the desegregation of interstate transportation. The ICC, which was established about 25 years before the FTC to regulate common carriers, had a mandate to combat unfairness writ large. Section 3 of the Interstate Commerce Act stated:

[I]t shall be unlawful for any common carrier subject to the provisions of this act to make or give any undue or unreasonable preference or advantage to any particular person, company, firm, corporation, or locality, or to subject any particular person, company, firm, corporation, or locality, or any particular description of traffic, to any undue or unreasonable prejudice or disadvantage in any respect whatsoever.<sup>423</sup>

Even though this provision did not explicitly mention discrimination, it was known as the “unjust discrimination” provision of the Act<sup>424</sup> and was most commonly used in cases regarding rate discrimination in interstate transportation and similar forms of commercial discrimination.<sup>425</sup> But the Supreme Court observed that “[t]his language is certainly sweeping enough to embrace all the discriminations of the sort described which it was within the power of Congress to condemn.”<sup>426</sup>

Indeed, “[f]rom the beginning, the Interstate Commerce Commission has recognized the application of that language to” race discrimination,<sup>427</sup> although the Supreme Court had to make the ICC properly follow through on the statutory mandate. For example, in 1937, U.S. Representative Arthur W. Mitchell, a Black resident of Chicago, paid a first-class fare to take a train to Hot Springs.<sup>428</sup> As the train crossed from Tennessee to

---

<sup>422</sup> See Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 *Antitrust L.J.* 1 (2003), <https://www.ftc.gov/sites/default/files/attachments/federal-trade-commission-history/origins.pdf>.

<sup>423</sup> Interstate Commerce Act, Pub. L. 49-104, 24 Stat. 379, 49th Cong. § 3 (1887).

<sup>424</sup> *Louisville & N. R. Co. v. United States*, 282 U.S. 740, 748 (1931).

<sup>425</sup> See, e.g., *Houston, E. & W.T. Ry. v. United States*, 234 U.S. 342 (1914) (“*The Shreveport Case*”).

<sup>426</sup> *Id.* at 356; see also *Boynton v. Virginia*, 364 U.S. 454, 457 (1960) (“The Interstate Commerce Act, as we have said, uses language of the broadest type to bar discriminations of all kinds.”).

<sup>427</sup> *Henderson*, 339 U.S. at 823 (collecting ICC cases).

<sup>428</sup> *Mitchell*, 313 U.S. 80.

Arkansas, he was forced to move from the first-class railcar into a “filthy and foul smelling” segregated car under threat of arrest.<sup>429</sup> He filed a complaint with the ICC alleging unfair discrimination, but lost. The ICC said demand by Black riders for the nicer accommodations was negligible and therefore this one refusal was not unjust or undue.<sup>430</sup> The Supreme Court reversed because “it cannot be maintained that the discrimination [because of his race] was not essentially unjust” or “deemed to lie outside the purview of the sweeping prohibitions of the Interstate Commerce Act.”<sup>431</sup> Moreover, the Court held, “*the comparative volume of traffic cannot justify the denial of a fundamental right of equality of treatment.*”<sup>432</sup>

Racial segregation and the ICC returned to the Supreme Court in *Henderson v. United States* in 1950.<sup>433</sup> In 1942, Elmer Henderson, a Black man traveling on a first-class ticket from Washington, D.C., to Birmingham, was denied an open seat in the dining car because white passengers were present. The ICC again ruled to uphold segregation. And the Supreme Court again held the segregation was an “undue or unreasonable prejudice or disadvantage” and rebuked the argument that “the limited demand for dining-car facilities” justified discrimination.<sup>434</sup> It held, “[I]t is no answer to the particular passenger who is denied service at an unoccupied place in the dining car that, on the average, persons like him are served.”<sup>435</sup> Through *Mitchell* and *Henderson*—both cases that originated in the ICC—the Court reinforced one of the central pillars of civil rights laws: that if services are being provided, equal treatment is required regardless of aggregate demand.

By the 1950s, the ICC helped advanced desegregation without the Court’s intervention. In 1952, Sarah Keys, a private in the Women’s Army Corps, was arrested after she refused to give up her seat at the front of a bus to a white Marine as she traveled

---

<sup>429</sup> *Id.* at 90–91.

<sup>430</sup> *Id.* at 91–92.

<sup>431</sup> *Id.* at 94; *see also id.* at 95 (collecting ICC cases concerning race discrimination).

<sup>432</sup> *Id.* at 97 (emphasis added).

<sup>433</sup> 339 U.S. 816 (1950).

<sup>434</sup> *Id.* at 825.

<sup>435</sup> *Id.*

through North Carolina.<sup>436</sup> The ICC held for the first time in *Keys v. Carolina Coach Co.* that the Interstate Commerce Act prohibited segregation on interstate buses.<sup>437</sup>

The Interstate Commerce Act and the holdings arising from it had a significant impact on the development of integral civil rights laws. In 1960, in *Boynton v. Virginia*, the Supreme Court extended the holdings of *Mitchell* and *Henderson*. It held the Interstate Commerce Act prohibited race discrimination as an unfair practice in other services and facilities related to interstate bus and rail travel, including terminals and restaurants in them.<sup>438</sup> *Boynton* launched the Freedom Rides in 1961, in which civil rights activists tested the decision by riding integrated buses through the Deep South. The resulting violence against the Freedom Riders appalled the nation and led directly to the integration of places of public accommodation, particularly restaurants and transportation facilities, in Title II of the Civil Rights Act of 1964.

## **VI. Effective rules must prohibit discriminatory commercial surveillance practices.**

This section responds to a series of the ANPR's questions about targeted advertising (questions 39, 40, 41, and 62), automated decision-making systems (questions 53, 55, 61, 65, and 66), and biometric information (questions 37 and 38).<sup>439</sup> In brief, targeted advertising is an inherently discriminatory and unfair trade practice that the Commission should prohibit. Targeted advertising segregates by nature and is in many ways the modern version of "separate but equal." Automated decision-making systems perpetuate systemic bias and often erode core federal protections against discrimination. Accordingly, automated decision-making systems that carry substantial risk of denial of civil rights protection or equal opportunity should be subject to pre- and post-deployment impact assessments. The Commission should also restrict the use of biometric technologies, such as facial recognition, which are often discriminatory and result in unfairness.

### **A. Targeted advertising is an unfair trade practice.**

Targeted advertising causes substantial and discriminatory harms because it segregates consumers, often according to protected characteristics. This segregation is itself

---

<sup>436</sup> See T. Anthony Bell, *The quietly defiant, unlikely fighter: Pfc. Sarah Keys and the fight for justice and humanity*, U.S. Army (Feb. 25, 2014), [https://www.army.mil/article/120456/The quietly defiant unlikely fighter Pfc Sarah Keys and the fight for justice and humanity/](https://www.army.mil/article/120456/The_quietly_defiant_unlikely_fighter_Pfc_Sarah_Keys_and_the_fight_for_justice_and_humanity/).

<sup>437</sup> *Keys v. Carolina Coach Co.*, 64 MCC 769 (1955).

<sup>438</sup> *Boynton*, 364 U.S. 454.

<sup>439</sup> ANPR, 87 Fed. Reg. at 51283–84.

discriminatory and imposes stigmatic harm, independent of an accompanying economic injury.<sup>440</sup> However, targeted advertising also imposes economic harm by restricting opportunities and promoting misinformation on the basis of protected characteristics. Consumers cannot reasonably avoid the discriminatory impacts of targeted advertising because they have no way to detect discriminatory advertising or meaningfully compare the ads they receive with the ads that others receive. And there is no offsetting benefit to consumers or competition to outweigh the harms of targeted advertising. Thus, the Commission has authority to regulate—and should regulate—targeted advertising as an unfair trade practice.

### 1. Targeted advertising defined.

Targeted advertising relies on the collection of overwhelming amounts of data points on consumers, including age, gender, place of residence and prior residences, employment and education history, family members, relationships, and much more.<sup>441</sup> Many sites collect data that the user does not volunteer through extensive tracking and

---

<sup>440</sup> See, e.g., *Heckler*, 465 U.S. at 750 (finding that the United States could not impose certain sex-based differences in processing pension benefits for spouses under Social Security based on archaic stereotypes that a man was less likely than a woman to rely on his spouse for economic support); *McLaurin*, 339 U.S. at 640–41 (holding that segregation “impair[s] and inhibit[s]” segregated students despite the segregated students’ ability to use “the same classroom, library, and cafeteria as students of other races” without indication of “any disadvantage”); *Henderson*, 339 U.S. at 824 (finding dining car segregation unlawful even though railway offered alternative dinner service to excluded Black patron for no extra charge).

<sup>441</sup> See, e.g., Rena Bivens & Oliver L. Haimson, *Baking Gender into Social Media Design: How Platforms Shape Categories for Users and Advertisers*, Soc. Media + Soc’y (2016), <https://journals.sagepub.com/doi/epub/10.1177/2056305116672486>; Twitter, *About Age Screening on Twitter*, <https://help.twitter.com/en/safety-and-security/age-verification> (last visited Nov. 8, 2022); TikTok, *Guardian’s Guide*, <https://www.tiktok.com/safety/en/guardians-guide/> (last visited Nov. 8, 2022); Pavni Diwanji, *How Do We Know Someone Is Old Enough to Use Our Apps?*, Meta (July 27, 2021), <https://about.fb.com/news/2021/07/age-verification/>; Facebook, *Ad Preferences* (last visited Nov. 8, 2022), [https://www.facebook.com/help/109378269482053/?helpref=hc\\_fnav](https://www.facebook.com/help/109378269482053/?helpref=hc_fnav) (last visited Nov. 8, 2022).

third parties.<sup>442</sup> These data are used to profile and classify people,<sup>443</sup> compare them to other people's profiles, and try to find hidden correlations.<sup>444</sup>

Targeted advertising then proceeds in two stages: targeting and delivery. In the targeting stage, advertisers and ad platforms work together to identify whom to target.<sup>445</sup> Targeting can rely on ad segments, custom audiences, direct targeting of gender or location, or "lookalike audiences."<sup>446</sup> While businesses may employ different processes to identify whom to target, the end result is used is an "eligible audience": the universe of people "eligible" to receive the ad.<sup>447</sup> In many instances, the eligible audience may already exclude protected groups of people, for example, if an ad is targeting only men over 35.

Next, algorithmic processes determine which individuals within the eligible audience will actually receive the ad. Due to limited ad space, not every member of the eligible audience will see the targeted ad. The algorithms optimize for responsiveness and rebalance in real time based on who is responding to an ad. Facebook's algorithm, for example, "decide[s] which users will see an ad" by "consider[ing] sex and close proxies for the other protected classes. . . . [Facebook] alone, not the advertiser, determines which

---

<sup>442</sup> See, e.g., Brian X. Chen & Daisuke Wakabayashi, *You're Still Being Tracked on the Internet, Just in a Different Way*, N.Y. Times (Apr. 6, 2022), <https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html>; Gabriel J.X. Dance et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.

<sup>443</sup> See Jeannie Marie Paterson et al., *The Hidden Harms of Targeted Advertising by Algorithm and Interventions from the Consumer Protection Toolkit*, 9 Int'l J. on Consumer L. & Prac. 1, 3–4 (2021).

<sup>444</sup> See Sebastian Sevignani, *Surveillance, Classification, and Social Inequality in Informational Capitalism: The Relevance of Exploitation in the Context of Markets in Information*, 42 Hist. Soc. Rsch. 77, 81–82 (2017); see also Kofman & Tobin, *supra* note 121; Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, Harv. Bus. Rev. (Nov. 8, 2019), <https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias>.

<sup>445</sup> Sevignani, *supra* note 444, at 83–84.

<sup>446</sup> See, e.g., Meta, *Ad Targeting*, <https://www.facebook.com/business/ads/ad-targeting> (last visited Nov. 8, 2022); Google, *About Audience Targeting*, <https://support.google.com/google-ads/answer/2497941?hl=en> (last visited Nov. 8, 2022).

<sup>447</sup> See, e.g., Complaint at 2, *United States v. Meta Platforms, Inc.*, No. 1:22-cv-05187 (S.D.N.Y. June 21, 2022) (alleging that Meta's ad delivery system used Fair Housing Act-protected characteristics to determine the "eligible audience").

users will constitute the ‘actual audience’ for each ad.”<sup>448</sup> This ad delivery system will target users with characteristics the algorithm deems most likely to engage with the content, even if an advertiser aims to target across a broad range of protected classes.<sup>449</sup>

Unlike contextual advertising, which is “an automated process where a promotional message is matched to relevant digital content,”<sup>450</sup> algorithmic discrimination is inherent in targeted advertising. If targeted ad platforms used contextual advertising, they would match ads to content posted on its website such that every user viewing the same piece of content would see the same ad. Users would have more control over what ads they receive because they have more control over what content they choose to view. Instead of merely delivering ads based on the content they run alongside—as TV, radio, and newspapers have done for decades—targeted advertising systems deliver ads based on the personal traits of its users, including their protected characteristics.

Targeted advertising is prevalent. The U.S. market for digital advertising was estimated at \$155.3 billion in 2021 and is projected to be worth \$786.2 billion by 2026.<sup>451</sup> The advertising market is dominated by a handful of major firms who have claimed a growing share of the advertising market by leveraging their ability to segment and target their userbases. Google, Meta, and Amazon are on track to generate over 50% of all advertising revenue in 2022.<sup>452</sup> Thus, a small number of companies perpetuate algorithmic discrimination in targeted advertising, yet almost every American consumer feels the impact.

---

<sup>448</sup> Charge of Discrimination at 5, *U.S. Dep’t of Hous. and Urban Dev. v. Facebook, Inc.*, FHEO No. 01-18-0323-8, at 4 (Mar. 28, 2019).

<sup>449</sup> See *id.*; Ali et al., *supra* note 121, at 13 (“Facebook’s ad delivery process can significantly alter the audience the ad is delivered to compared to the one intended by the advertiser based on the content of the ad itself.”).

<sup>450</sup> James Chen, Contextual Advertising, Investopedia (Apr. 18, 2021), <https://www.investopedia.com/terms/c/contextual-advertising.asp>.

<sup>451</sup> ReportLinker, *Global Digital Advertising and Marketing Market to Reach \$786.2 Billion by 2026*, GlobeNewswire (May 4, 2022), <https://www.globenewswire.com/news-release/2022/05/04/2435674/0/en/Global-Digital-Advertising-and-Marketing-Market-to-Reach-786-2-Billion-by-2026.html>.

<sup>452</sup> Seb Joseph & Ronan Sheilds, *The Rundown: Google, Meta and Amazon Are on Track to Absorb More Than 50% of All Ad Money in 2022*, Digiday (Feb. 4, 2022), <https://digiday.com/marketing/the-rundown-google-meta-and-amazon-are-on-track-to-absorb-more-than-50-of-all-ad-money-in-2022/>.

## 2. Targeted advertising causes substantial injury to consumers through segregation-based discrimination.

The Commission asks in question 11 about business models that incentivize harmful practices. Targeted advertising depends on exclusionary business models that segregate users and encourage toxic content such as election disinformation. In question 12, the Commission asks how harms to different classes of consumers should be addressed. Targeted advertising has a discriminatory effect on protected classes of people, including based on race, gender, and age. The exclusionary nature of targeted advertising perpetuates harmful stereotypes and excludes members of these protected classes from economic opportunities. It also encourages business models that result in negative externalities.

First, targeted advertising segregates by definition and is fundamentally exclusionary. Indeed, a key aspect of targeted ads is that they are usually visible “only . . . to their intended targets,” which by nature excludes particular groups of people.<sup>453</sup> Moreover, when ads are targeted to groups using specific protected characteristics, or proxies for those characteristics, user bases are effectively segregated. This segregation, in turn, ushers in a new era of “separate but equal.” Even when protected classes of people are not purposefully excluded from a specific advertisement, advertisers and ad networks use criteria or algorithms that cause disparate impacts by having the effect of segregating consumers based on protected characteristics. Automated decision-making systems used in advertising often rely on biased data that perpetuates inequality and reinforces the existing marginalization of individuals or groups.<sup>454</sup> This frustrates the intent and purpose of decades of civil rights statutes and regulations at the state and federal level, as well as the tireless efforts of generations of civil rights activists and community leaders to try to close racial disparities and promote equal opportunity.

When targeted ad platforms apply algorithms to the data of their chosen audience, the algorithms create efficiency by finding hidden correlations—they see that older Black women, for example, are less likely to be wealthy, to live in an expensive neighborhood, to have a graduate degree, to have job security, or to be adequately insured—and the algorithms mistake the *consequences* of historical discrimination for the *preferences* of older Black women. The algorithms segregate users based upon immutable traits or proxies thereof, and provide different service on that basis.

---

<sup>453</sup> Nicholas Carah et al., *How Dark Is ‘Dark Advertising’? We Audited Facebook, Google and Other Platforms to Find Out*, The Conversation (Sept. 6, 2022), <https://theconversation.com/how-dark-is-dark-advertising-we-audited-facebook-google-and-other-platforms-to-find-out-189310>.

<sup>454</sup> See Paterson et al., *supra* note 443, at 3–4.

This segregation, whether caused by disparate treatment or resulting in disparate impact, imposes greater burdens on some people to access jobs, housing, or other opportunities. The additional time, money, effort, or humiliation incurred to overcome that hurdle is an injury<sup>455</sup>—just like when a restaurant serves Black patrons at the kitchen window while white patrons receive table service.<sup>456</sup> Indeed, targeted advertising has prevented protected classes of people, particularly Black Americans and other people of color, from accessing housing, credit, employment, and other core opportunities that legislation like the Fair Housing Act and the Civil Rights Act seek to guarantee.<sup>457</sup> These harms cannot be justified by the argument that targeted advertising discriminates against everyone or by an argument that relies on the aggregate demand for the service.<sup>458</sup> Simply put, segregating advertisements for economic opportunities on the basis of protected characteristics is unfair discrimination.<sup>459</sup>

Second, targeted advertising incentivizes business models that maximize user engagement, and these business models in turn cause negative externalities. Platforms have an incentive to maximize user engagement at all costs, so that users spend more time on the platform and see more ads, which leads to more profits.<sup>460</sup> Social media networks and hosts of ad-supported user-generated content design algorithms to recommend content that maximizes user engagement, regardless of whether that content is harmful in other ways.<sup>461</sup> For example, this results in companies' amplification of white supremacist content and content that is harmful and addictive to teenagers and children.<sup>462</sup>

---

<sup>455</sup> See *Ne. Fla. Chapter of Associated Gen. Contractors of Am*, 508 U.S. at 666 (holding that making it harder for one group to obtain an opportunity, even without a formal barrier, constitutes an injury in fact).

<sup>456</sup> See *Newman v. Piggie Park Enter., Inc.*, 377 F.2d 433, 434 n.3 (4th Cir. 1967), *aff'd* 390 U.S. 400 (1968).

<sup>457</sup> See *supra* § III.

<sup>458</sup> See *supra* § IV.A.3.

<sup>459</sup> See *Pittsburgh Press*, 413 U.S. at 377–78 (upholding ordinance prohibiting sex-segregated employment ads in a newspaper classifieds section); *Ragin v. N.Y. Times Co.*, 923 F.2d 995, 998 (2d Cir. 1991) (holding that the Fair Housing Act applied to a newspaper's use of models in advertisements as an expression of racial preferences).

<sup>460</sup> See Michael Ashley, *Sick of the Attention Economy? It's Time to Rebel*, *Forbes* (Nov. 24, 2019), <https://www.forbes.com/sites/cognitiveworld/2019/11/24/sick-of-the-attention-economy-its-time-to-rebel/?sh=2b6323c535ac>.

<sup>461</sup> See *id.*

<sup>462</sup> See *supra* § III.E & H.

Targeted advertising also results in particularly harmful externalities concerning election interference and misinformation. Section III above describes examples such as Facebook rolling back measures they put in place to combat misinformation and YouTube recommending election fraud conspiracy theories to users predisposed to be skeptical of election results.<sup>463</sup> As discussed above, the Russian campaign to interfere in the 2016 election used off-the-shelf targeted advertising tools. Additionally, as described in Section III, those looking to influence elections can target specific demographics—either directly or by targeting proxies such as narrowly drawn locations—who may be more inclined to fall for specific pieces of disinformation.<sup>464</sup>

### **3. Consumers cannot reasonably avoid targeted advertising.**

Consumers cannot reasonably avoid targeted advertising because the nature of targeted advertising makes it difficult for users to discover that they are being targeted with ads. Even when they are aware that they are seeing targeted ads, it is often impossible for consumers to discover the ads on which they are missing out. Moreover, consumers are powerless to set the terms on which targeted advertisements are delivered to them. And, as discussed above and in *Napleton Auto*, consumers cannot change their immutable characteristics.<sup>465</sup>

First, the nature of targeted advertising makes it difficult for users to discover that they are being delivered targeted ads in the first place. Not only are targeted ads usually visible “only to their intended targets,” but they are also difficult to track as they often disappear after a user leaves a web page or continues to scroll down their feed.<sup>466</sup>

Second, even when consumers are aware they are seeing targeted ads, the exclusionary nature of targeted advertising makes it near impossible for consumers to notice or seek out the ads that other users are seeing. By definition, targeted ad platforms depend on each user having a different, personalized experience. Thus, users do not know when advertisers and advertising networks have excluded them from an ad for a credit card, discount sale, or affordable insurance plans because the feeds of other users are inaccessible. Without accessing the full breadth of available ads, consumers cannot tell when they are being denied opportunities available to other users.<sup>467</sup> For the same

---

<sup>463</sup> See *supra* § III.I.

<sup>464</sup> See *id.*

<sup>465</sup> See *Napleton Statement*, *supra* note 108, at 3.

<sup>466</sup> Carah et al., *supra* note 453.

<sup>467</sup> See Silvia Milano et al., *Epistemic Fragmentation Poses a Threat to the Governance of Online Targeting*, 3 *Nature Mach. Intel.* 466, 466–67 (2021).

reason, consumers cannot tell when they are being targeted with predatory or otherwise harmful advertising. This makes it increasingly difficult for consumers to identify how they are being targeted and what other economic opportunities might be available to them.

Ad libraries do not solve the fundamental unfairness of the targeted advertising system because consumers would need to make an affirmative effort to find their desired ads.<sup>468</sup> It is well established that having to do more effort to reach the same result is a significant cost. For instance, the Supreme Court has stated that “the imposition of [a] barrier” creates “the inability to compete on an equal footing.”<sup>469</sup> This is particularly true in the context of discrimination in economic opportunities. It is insufficient to provide mere access to opportunities to everyone when some people are treated better than others; the treatment, service, and access must be equal.<sup>470</sup> Thus, even imagining an ad library that is perfectly accessible, easy to use, contained every ad, and every consumer was perfectly adept at using it, it would still be inadequate because searching an ad library requires affirmative effort on the part of the consumer and therefore is necessarily less convenient than receiving ads directly. That is the whole point of the efficiency argument for advertising—if it was just as easy for consumers to look up opportunities for themselves, the economic value to the advertiser would be significantly diminished.

Third, users are unable set the terms on which targeted advertisements are delivered to them. Terms of service and privacy policies are no help. In the end, consumers have no choice but to accept the terms of service if they want to use essential Internet services. Moreover, it is unreasonable to expect consumers to understand how their data is used for targeted ads, figure out what options they have to opt-out of data collection,

---

<sup>468</sup> See Kate Kaye, *Facebook Is ‘Not a Researchers-Friendly Space’ Say Academics Encountering Roadblocks to Analyzing Its 2020 Election Ad Data*, Digiday (May 4, 2021), <https://digiday.com/marketing/facebook-is-not-a-researchers-friendly-space-say-academics-encountering-roadblocks-to-analyzing-its-2020-election-ad-data/>.

<sup>469</sup> *Ne. Fla. Chapter of Ass’n Gen. Contractors of Am.*, 508 U.S. at 666 (holding that making it harder for one group to obtain an opportunity, even without a formal barrier, constitutes an injury in fact and deprives equal opportunity).

<sup>470</sup> See *McLaurin*, 339 U.S. at 640 (holding segregation unlawful even when segregated student used “the same classroom, library, and cafeteria as students of other races” without indication of “any disadvantage”); *Henderson*, 339 U.S. at 818 (finding dining car segregation unlawful even though railway offered alternative dinner service to excluded Black patron at no extra charge); *Missouri ex rel. Gaines*, 305 U.S. at 349 (holding denial of service unlawful when “[t]he white resident is afforded legal education within the State” but a Black resident “having the same qualifications is refused it there and must go outside the State to obtain it”); *Jones v. Kehrlein*, 49 Cal. App. 646, 651 (Dist. Ct. App. 1920) (finding segregated theater seating unlawful even though theater provided access to the same show).

and then hold companies accountable for violations without outside intervention. Broadly worded consent-based privacy policies can deceive users by leaving them unable to anticipate when their data will be used for targeted ads. The majority of privacy policies exceed college reading level and can take at least 30 minutes to read.<sup>471</sup> Indeed, consumers are not reading these agreements—over 90% of consumers accept the “terms and conditions” of websites without reading them.<sup>472</sup>

#### **4. The benefits to consumers or competition do not outweigh the harms that targeted ads inflict.**

In questions 39, 40, and 41, the Commission inquires about the costs and benefits of limiting companies that profit from targeted advertising and potential alternative practices.<sup>473</sup> Any benefits of targeted advertising do not outweigh the exclusionary harm inherent in this system of advertising. Moreover, companies can turn to contextual advertising, which may be equally profitable.

Targeted advertising is inherently discriminatory, and the harms that have arisen from this business model are not outweighed by any benefits to consumers. While proponents of targeted ads may say that consumers prefer a personalized experience from their digital ads, these consumer preferences are based on stereotypes and narrow the opportunities made available to protected classes of people. As discussed above, similar arguments were raised in the past to defend segregation and have been repeatedly dismissed.<sup>474</sup>

Other forms of advertising may be equally effective as targeted advertising. Researchers have found that the influence of targeting advertising “may be exaggerated” and that “there remain ongoing concerns about the risk of harm to consumers [that targeted ads] may generate.”<sup>475</sup> Google has recently been accused of misleading

---

<sup>471</sup> Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. Times (June 12, 2019), <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>.

<sup>472</sup> Caroline Cakebread, *You’re Not Alone, No One Reads Terms of Service Agreements*, Bus. Insider (Nov. 15, 2017), <https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11>.

<sup>473</sup> ANPR, 87 Fed. Reg. at 51283.

<sup>474</sup> See *supra* § IV.A.3.

<sup>475</sup> Paterson et al., *supra* note 443, at 9.

advertisers about the prices and value of their ads.<sup>476</sup> One empirical study found that targeted ads only bring in about 4% more revenue than non-targeted ads.<sup>477</sup> Even the most rapidly growing and popular apps right now, such as TikTok, are not seeing high returns on targeted ads.<sup>478</sup>

Companies can turn to other forms of advertising to reach consumers that are less harmful than targeted advertising. Contextual ads, for example, are less likely to reinforce discrimination and incentivize harmful and deceptive business practices because contextual ads are not exclusionary. As explained above, contextual advertising matches a promotional message to relevant digital content rather than to characteristics of the user.<sup>479</sup> Thus, unlike targeted advertising, contextual advertising is not fundamentally exclusionary.

Because contextual ads are indexed to particular content—such as a banner on a website, a location for a billboard, a section in a newspaper, a break in a particular show—everyone who views that context sees the same ad.<sup>480</sup> For instance, an advertisement for perfume in an online fashion magazine does not differentiate among the different types of people who read online fashion magazines. Contextual advertising also allows consumers to better understand and debate both the reason they have been served a particular ad and the message of the ad itself. If ads are indexed to a site’s content, all visitors to the site would have the same context and therefore could recognize potentially harmful and misleading advertising.<sup>481</sup>

\* \* \*

---

<sup>476</sup> Tripp Mickle & Keach Hagey, *Google Misled Publishers and Advertisers, Unredacted Lawsuit Alleges*, Wall St. J. (Jan. 14, 2022), <https://www.wsj.com/articles/google-misled-publishers-and-advertisers-unredacted-lawsuit-alleges-11642176036>.

<sup>477</sup> Keach Hagey, *Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests*, Wall St. J. (May 29, 2019), <https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195>.

<sup>478</sup> Marc Bain, *The Returns on TikTok Ads Don’t Match the Hype Just Yet*, Bus. of Fashion (Aug. 22, 2022), <https://www.businessoffashion.com/articles/technology/the-returns-on-tiktok-ads-dont-match-the-hype-just-yet/>.

<sup>479</sup> Chen, *supra* note 450.

<sup>480</sup> See Hana Choi et al., *Online Display Advertising Markets: A Literature Review and Future Directions*, 31 Info. Sys. Rsch. 556, 560 (2020), <https://hanachoi.github.io/research-papers/choi-et-al-review-display-advertising.pdf>.

<sup>481</sup> See *id.*

In sum, the Commission should prohibit targeted advertising as an unfair trade practice that discriminates against particular classes of consumers, restricting opportunities and promoting harmful and divisive messages. Consumers cannot reasonably avoid these harms but advertisers and platforms can mitigate them simply by turning to equally effective but less discriminatory models of digital advertising.

**B. Unchecked use of automated decision-making systems is likely to result in discrimination and is an unfair trade practice.**

Automated decision-making systems carry an enhanced risk of significant injury to consumers and can erode civil rights protections or deny equal access to economic opportunities or government services. Given the “black box” nature of many automated decision-making systems that prevent the ability to explain how they make decisions, consumers cannot reasonably avoid these harms. And given that these harms involve discrimination and denial of equal opportunity, no countervailing benefits outweigh them. Again, as a threshold matter, if the Commission agrees that discrimination is an unfair trade practice,<sup>482</sup> then any use of automated decision-making systems that results in discrimination is necessarily an unfair trade practice, and consequently automated decision-making systems can only be permitted if they can be ascertained *not* to result in discrimination.

Because they place consumers at significant risk of discrimination or other harms, real-world deployment of automate decision-making systems without sufficient safeguards is an unfair trade practice. In the context of data security, the Commission has long held that it is an unfair trade practice for a firm to fail to take adequate precautions to secure personal data because lax security increases the risk of data breaches and exposes consumers to the risk of identity theft, fraud, discrimination, and other harms.<sup>483</sup> Automated decision-making systems necessitate a similarly precautionary approach.

The Commission should, by regulation, set such requirements—including but not limited to impact assessments—as well as require the disclosure of information about the datasets used to build, train, and operate the automated decision-making systems. The Commission should also implement the newly released *Blueprint for an AI Bill of Rights*

---

<sup>482</sup> See *supra* § IV.

<sup>483</sup> See ANPR, 87 Fed. Reg. at 51279 (collecting cases); Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* 224, 227, 234 (2016) (collecting cases); see also *supra* § V.B.

developed by the White House Office of Science and Technology Policy.<sup>484</sup> Specifically, the Commission should propose rules implementing the five principles in the AI Bill of Rights for responsible use of automated decision-making systems: (1) safe and effective systems; (2) algorithmic discrimination protections; (3) data privacy; (4) notice and explanation; and (5) human alternatives, consideration, and fallback.<sup>485</sup>

**1. Automated decision-making systems place consumers at risk of substantial injury.**

In this section we respond to questions 55, 65, and 66, noting that the overstated reliability of automated decision-making systems has the potential to lead to greater consumer harms when there are algorithmic errors, and algorithmic discrimination in particular is prevalent.<sup>486</sup> Indeed, federal policymakers have been concerned about “the potential of encoding discrimination in automated decisions” for a long time.<sup>487</sup> The Commission has shared this concern, identifying the creation or reinforcing of existing disparities or the creation of new justifications for exclusion as two primary risks of increased use of “big data.”<sup>488</sup> The Commission went further in April 2021, where it advised that the sale or use of racially biased algorithms was an unfair and deceptive trade practice under Section 5 of the FTC Act.<sup>489</sup> The Office of Science and Technology Policy’s recent *Blueprint for an AI Bill of Rights* also discusses the potential harms from unregulated use of automated decision-making systems at length.<sup>490</sup>

Concerns about algorithmic discrimination have mounted as the use of “big data” has intensified. Machine learning algorithms, artificial intelligence (“AI”), and other automated decision systems have insinuated themselves into nearly every sector. A recent market research study has pegged the value of the current global “AI market” at nearly

---

<sup>484</sup> See White House Off. of Sci. & Tech. Pol’y, *Blueprint for an AI Bill of Rights* (2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf> [hereinafter *Blueprint*].

<sup>485</sup> *Id.* at 5–7.

<sup>486</sup> ANPR, 87 Fed. Reg. at 51283–84.

<sup>487</sup> See Exec. Off. of the President, *supra* note 116.

<sup>488</sup> See FTC, *Big Data: A Tool for Inclusion or Exclusion?*, *supra* note 301, at 10 (2016).

<sup>489</sup> Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company’s Use of AI*, FTC (Apr. 19, 2021), <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

<sup>490</sup> See *Blueprint*, *supra* note 484, at 16–17.

\$60 billion, with the expectation that this market will grow to \$422.37 billion by 2028.<sup>491</sup> The federal government has encouraged this unchecked growth, with the National AI Initiative Act seeking to create “a coordinated program across the entire Federal government to accelerate AI research and application for the Nation’s economic prosperity and national security.”<sup>492</sup>

The growing use of AI has resulted in significant harms to the individuals and communities bearing the consequences of automated decisions, often on the basis of race or other characteristics.<sup>493</sup> Even when race or other personal characteristics are not explicitly part of algorithmic decisions, they can creep into these decisions via proxies.<sup>494</sup> At their worst, automated decisions can undermine public laws and policies designed expressly to prevent discrimination. And even where no such law or policy provides a background principle, consumers face substantial harms that this Commission is charged with preventing. These harms occur in numerous sectors, including housing, employment, access credit and finance, insurance, public health and healthcare, education, public accommodations, government benefits, and policing.<sup>495</sup> They also facilitate, directly or indirectly, negative externalities related to online hate and harassment, voter suppression, and disinformation.<sup>496</sup>

## **2. Consumers cannot reasonably avoid harms from discriminatory automated decision-making systems.**

Consumers are unable to avoid the risk of substantial injury posed by unbounded automated decision systems for the same reasons that consumers are unable to avoid the risk identified by the Commission in its complaint against Kochava’s sharing of

---

<sup>491</sup> Zion Mkt. Rsch., *\$422.37+ Billion Global Artificial Intelligence (AI) Market Size Likely to Grow at 39.4% CAGR During 2022-2028*, Bloomberg Newswire (June 27, 2022), <https://www.bloomberg.com/press-releases/2022-06-27/-422-37-billion-global-artificial-intelligence-ai-market-size-likely-to-grow-at-39-4-cagr-during-2022-2028-industry>.

<sup>492</sup> Nat’l A.I. Initiative, <https://www.ai.gov/> (last visited Sept. 27, 2022).

<sup>493</sup> See *supra* § III.

<sup>494</sup> See Omer Tene & Jules Polonetsky, *Taming the Golem: Challenges of Ethical Algorithmic Decision-Making*, 19 N.C.J.L. & Tech. 125, 136 (2017) (“Even if a particular attribute is not present in the data, combinations of other attributes can act as a proxy. Algorithmic parameters are never neutral. They are always imbued with values.” (citation omitted)).

<sup>495</sup> See *supra* § III.A–G, J–K.

<sup>496</sup> See *supra* § III.H & I.

geolocation data: their operations are entirely opaque to consumers.<sup>497</sup> Indeed, sophisticated machine learning models are often called “black boxes” because only their inputs and outputs are subject to view.<sup>498</sup> And the model or selection of inputs and outputs may be wrapped up in trade secrecy.<sup>499</sup> Even for data scientists and engineers, explaining how AI systems work is challenging. The recently published *Blueprint for an AI Bill of Rights* notes that the National Institute of Standards and Technology (“NIST”) and the Defense Advanced Research Projects Agency are conducting fundamental research and launching new programs to develop more explainable AI models.<sup>500</sup> Even if such models are in place, consumers should not bear the responsibility of policing the systems making decisions about them. We do not expect consumers to understand how an internal combustion engine works and blame the consumer if their car is a lemon. Instead we hold companies responsible when they negligently design their products.<sup>501</sup>

It is unrealistic and unfair to expect consumers to avoid automated decision-making when they either do not know that they have been subjected to it or could not explain how the decision affects them. The opacity and prevalence of automated decision-making systems, and the attendant risk of substantial injury to consumers, warrant the Commission’s intervention.

**3. No countervailing benefits to consumers or competition outweigh the harms inflicted by discriminatory automated decision-making systems.**

In question 53, the ANPR asks about the benefits of allowing companies to employ automated decision-making systems in critical areas, such as housing, credit, and employment.<sup>502</sup> In short, the Commission should scrutinize claimed benefits and not

---

<sup>497</sup> Complaint for Permanent Injunction and Other Relief at 9, *FTC v. Kochava, Inc.*, No. 2:22-cv-377 (D. Idaho Aug. 29, 2022); see also, e.g., *Passport Auto. Grp. Statement*, *supra* note 108, at 2 (noting consumers could not avoid injury “because they typically had no way of knowing they were being charged more than their White counterparts”); *Napleton Statement*, *supra* note 108, at 3–4 (noting that discrimination is unfair in part because it is unavoidable).

<sup>498</sup> Frank Pasquale, *The Black Box Society* 3 (2015).

<sup>499</sup> See Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 *UCLA L. Rev.* 54, 99 (2019).

<sup>500</sup> See *Blueprint*, *supra* note 484, at 45.

<sup>501</sup> See, e.g., *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021) (Social media company not immune from liability for negligent design when its app prompted users to travel at high speeds and a user got in a car accident as a result.)

<sup>502</sup> ANPR, 87 Fed. Reg. at 51283.

countenance efficiency gains of automated decision-making systems when those gains come at the expense of the accuracy, reliability, and fairness of the decisions made.<sup>503</sup> There may be parochial benefits to the companies that design the systems or the companies that use them to replace human decision-makers, but those benefits should not be given undue weight in the Commission’s analysis if they come at the cost of depriving consumers of core civil rights protections or cause harm to the public interest.<sup>504</sup> Further, it is unclear that the companies and government agencies using the systems truly benefit if the systems they rely on consistently produce unreliable or unlawfully discriminatory decisions.

**4. The Commission should implement the *AI Bill of Rights* and require pre- and post-deployment impact assessments.**

In questions 56, 61, and 67, the Commission asks what specific steps it should take to prevent algorithmic errors and what rules it should adopt to limit the deployment of systems that produce discrimination.<sup>505</sup> The Commission should do two things: (1) implement the recommendations of the *AI Bill of Rights*, and (2) require pre- and post-deployment impact assessments. Deployment of an automated decision-making system in real-world conditions without satisfying these requirements should be declared an unfair trade practice.

The answer begins with the recently announced *AI Bill of Rights*, which articulates five principles to “help provide guidance whenever automated systems can meaningfully impact the public’s rights, opportunities, or access to critical needs.”<sup>506</sup> Those principles are: safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and human consideration and fallback.<sup>507</sup> Moreover, as the *AI Bill of Rights* highlights, sometimes the best course of action is to *not* use an automated system or to decommission an existing system that is causing harm.<sup>508</sup> The Commission should use these principles to design regulatory requirements to mitigate the potential harmful impacts of automated decision-making systems.

In particular, the Commission should require algorithmic impact assessments that test for both discriminatory biases and other significant risks of harm. As the *AI Bill of*

---

<sup>503</sup> See *supra* § IV.A.3.

<sup>504</sup> *Id.*

<sup>505</sup> ANPR, 87 Fed. Reg. at 51283–84.

<sup>506</sup> *Blueprint*, *supra* note 484, at 5–7.

<sup>507</sup> *Id.*

<sup>508</sup> *Id.* at 18.

*Rights* explains, “[i]ndependent evaluation and plain language reporting in the form of an algorithmic impact assessment, including disparity testing results and mitigation information, should be performed and made public whenever possible to confirm these protections [against algorithmic discrimination].”<sup>509</sup>

Impact assessments should occur at two points in time—before and after deployment—and should be a two-step process each time. Pre-deployment assessments should occur both before initial deployment of a system and before any material change to the system. Post-deployment assessments should occur at regular intervals depending on the nature of the system, but at least annually, as well as after material changes.

The first step of the two-step process should apply to every automated decision-making system being used in connection with important sectors such as housing, employment, credit and finance, insurance, healthcare, education, public accommodations, utility service, government benefits or services, and policing. At this first step, both pre- and post-deployment, a company should conduct a light-touch evaluation to determine whether the automated decision-making system causes or materially contributes to a potential risk of injury to consumers. While all injuries should be considered, there should be a particular examination of the risk of discrimination and risks to vulnerable populations like children, the elderly, or low-income communities. If there is no potential risk, then no further assessment is necessary at that time. If yes, then the company should proceed to step two.

At step two, the company should conduct a detailed and comprehensive assessment. The Commission can look to several sources to determine how to craft these assessments, including the *AI Bill of Rights*, the American Data Privacy and Protection Act bill (“ADPPA”),<sup>510</sup> and the Algorithmic Justice and Online Platform Transparency Act bill (“AJOPTA”).<sup>511</sup> The Commission can also draw from multi-agency and interdisciplinary efforts like NIST’s development of an AI Risk Management Framework.<sup>512</sup> Civil society organizations such as AI Now have developed frameworks for algorithmic impact assessments for public agency use of automated decision-making systems that include both pre-

---

<sup>509</sup> *Id.* at 5.

<sup>510</sup> See H.R. 8152 § 207(c).

<sup>511</sup> S. 1896, Algorithmic Justice and Online Platform Transparency Act, § 4(a)(2)(A)(iv), 117th Cong., 1st Sess. (2021).

<sup>512</sup> See *AI Risk Management Framework: Second Draft*, Nat’l Inst. of Standards & Tech. (Aug. 18, 2022), <https://www.nist.gov/document/ai-risk-management-framework-2nd-draft>.

acquisition and post-deployment reviews.<sup>513</sup> The trade association BSA has also developed a framework for assessing bias in algorithms.<sup>514</sup>

In step two of a pre-deployment assessment, a firm should evaluate the design and structure of the system, potential biases that can arise, the data inputs and outputs (including the quality of training data), how the system is intended to be used and how it is likely to be used, how to mitigate biases and prevent harms, and other appropriate risk management considerations. Again, there should be a distinct consideration of likely impacts on the basis of protected characteristics and across vulnerable populations. Particular care should be paid to intersectional identities, such as women of color and LGBTQ people of color, as systems may compound multiple forms of discrimination. The output of the assessment should be a clear determination that either (1) the system is not likely to cause harm; (2) the firm is implementing mitigations to prevent harms; or (3) the firm will not deploy the system because the harms cannot be sufficiently mitigated.

In step two of a post-deployment assessment, a firm should measure what actually happened. Some of the questions the assessment should ask: Did the system function as intended and was it used as intended? Did it cause discrimination, including both disparate treatment or disparate impact? Did it cause other harms, such as privacy vulnerabilities? If the assessment identifies problems, it should also identify proposed solutions and mitigations – and the decommissioning of the system should always be an option if problems cannot be resolved.

It is particularly important that these assessments be conducted by independent third-party auditors and the assessment reports should be produced to the Commission. The Commission's rules regarding assessment transparency should accommodate the need to protect intellectual property and privacy, while also maximizing and encouraging transparency. This can be accomplished by requiring firms to publish the overall findings of their assessments without revealing sensitive information.

**C. Biometric technologies pose unique risks of harmful discrimination. Facial recognition is an unfair trade practice.**

The Commission seeks comment, in questions 37 and 38, on how companies collect and use biometric information, the benefits and harms of these practices, and whether the Commission should limit practices that facilitate the use of facial recognition,

---

<sup>513</sup> Dillon Reisman et al., *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*, AI Now (Apr. 2018), <https://ainowinstitute.org/aiareport2018.pdf>.

<sup>514</sup> BSA, *Confronting Bias: BSA's Framework to Build Trust in AI*, <https://ai.bsa.org/wp-content/uploads/2021/06/2021bsaaibias.pdf> (last visited Nov. 11, 2022).

fingerprinting, and other biometric technologies.<sup>515</sup> In this section we address those questions and make responsive recommendations to the Commission.

We are guided in part by the modern legal forefathers of privacy, Samuel Warren and Louis Brandeis: “If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression.”<sup>516</sup>

We urge the Commission to (1) propose rules for biometric technologies that are similar to other algorithmic technologies—namely, that such technologies must be tested pre-deployment for safety and efficacy and routinely audited for harmful impacts post-deployment; and (2) declare that the use of facial recognition technology (“FRT”) in certain types of “high risk settings,” as well as in public without explicit opt-in consent, is an unfair trade practice.

Many biometric technologies, such as facial recognition, have been shown to result in, or have the potential to result in, intentional discrimination and/or discriminatory disparate impacts. Moreover, even if a tool is facially neutral that does not mean it is incapable of harm. No matter how complex a biometric technology is, it remains a tool in the hands of those who wield it. When a technology is used to make a discriminatory system more efficient, that is a discriminatory use of the technology because it increases the quantity or quality of harm. Researchers have noted that such technologies “present a veneer of social control or risk mitigation,” while in reality they “tend to reproduce, maintain, and naturalize structural inequalities . . . and allow policymakers to avoid necessary structural reforms.”<sup>517</sup> “Use of digital technologies—including . . . biometric technology . . . have introduced new vectors to continue the deeply rooted historical exploitation of and discrimination against protected classes.”<sup>518</sup> “Baked into the mathematical formulas of the algorithm, represented by lines of code, are legacies of racist public policy and

---

<sup>515</sup> ANPR, 87 Fed. Reg. at 51283.

<sup>516</sup> Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 206 (1890).

<sup>517</sup> Stefanie Coyle & Rashida Richardson, *Bottom-Up Biometric Regulation: A Community’s Response to Using Face Surveillance in Schools*, in *Regulating Biometrics: Global Approaches and Open Questions* 104, 104 (Amba Kak ed., Sept. 2, 2020), <https://ainow-institute.org/regulatingbiometrics-coyle-richardson.pdf>.

<sup>518</sup> Erin Simpson & Adam Conner, *How To Regulate Tech: A Technology Policy Framework for Online Services*, Ctr. for Am. Progress (Nov. 16, 2021), <https://www.american-progress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/>.

discrimination dating back to the foundation of this country, codified through existing data sets as if they were digital artifacts of the past.”<sup>519</sup>

To address biometric technology, the Commission must first define the term “biometric information.” Its definition should be expansive and illustrative to include future technologies and avoid the potential for gamesmanship. The Illinois Biometric Information Privacy Act defines “biometric information” as an umbrella term for “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.”<sup>520</sup> The California Consumer Privacy Act defines it as “an individual’s physiological, biological, or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity.”<sup>521</sup> The American Data Privacy and Protection Act bill, which is currently pending in the U.S. House of Representatives, defines “biometric information” similarly to California and provides several non-exhaustive examples: fingerprints; voice prints; iris or retina scans; facial or hand mapping, geometry, or templates; and gait or personally identifying physical movements.<sup>522</sup> The Commission should use these authorities as a starting point but should focus on ensuring any definition can evolve with new technologies.

Biometric technologies can directly or indirectly result in discrimination through their design or through the datasets used to train their algorithms. These technologies are used in various ways, each of which carries risks of discrimination. Some technologies are used to identify or verify the identities of individuals, such as facial recognition. Others are used to make decisions about whether individuals will receive particular opportunities, such as technologies used to make eligibility determinations for jobs or healthcare.<sup>523</sup>

The reliability and risk of bias in biometric technology varies greatly depending on the design of the technology and the biometric marker being analyzed. One significant factor in determining reliability and risk of bias is the representativeness of the data set, including how the data was collected and how it is used. For example, criminal DNA

---

<sup>519</sup> Yeshimabeit Milner & Amy Traub, *Data Capitalism + Algorithmic Racism*, Data for Black Lives & Demos (May 17 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).

<sup>520</sup> Illinois’ Biometric Information Privacy Act, 740 Il. Comp. Stat. Ann. 14/10.

<sup>521</sup> Cal. Civ. Code § 1798.140.

<sup>522</sup> H.R. 8152 § 2(3)(A).

<sup>523</sup> See generally P. Jonathon Phillips et al., *An Introduction to Evaluating Biometric Systems* 56, U.S. Dep’t of Com. Nat’l Inst. of Standards & Tech. (2000), [https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=151436](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151436).

databases over-represent Black people,<sup>524</sup> while medical research DNA databases over-represent white people.<sup>525</sup> This is not a serendipitous coincidence. Black communities are over-policed in a systemic and discriminatory manner, which leads to more arrests of Black people, which leads to more Black DNA samples in the criminal databases.<sup>526</sup> White communities have greater access to healthcare and insurance,<sup>527</sup> as well as higher enrollment rates in research universities, which often use students as research subjects.<sup>528</sup> This disparity in access to healthcare and education is a downstream consequence of the legacies of redlining and segregation.<sup>529</sup> When data are drawn from sources affected by systemic racism, and then those data are used to produce models or other technologies,

---

<sup>524</sup> Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 Cal. L. Rev. 1847 (Dec. 2020), <https://www.californialawreview.org/print/racial-composition-forensic-dna-databases/>.

<sup>525</sup> Vicky Stein, *Genetic research has a white bias, and it may be hurting everyone's health*, PBS NewsHour (Mar. 22, 2019), <https://www.pbs.org/newshour/science/genetic-research-has-a-white-bias-and-it-may-be-hurting-everyones-health>.

<sup>526</sup> See, e.g., Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 Calif. L. Revi. 1847, 1851 (2020) (“DNA has been collected from Black persons at two and a half times the rate of White persons.”); Aaron Chalfin et al., *Police Force Size and Civilian Race* 11–12 (Nat’l Bureau of Econ. Rsch., Working Paper No. 28202, 2020), [https://www.nber.org/system/files/working\\_papers/w28202/w28202.pdf](https://www.nber.org/system/files/working_papers/w28202/w28202.pdf) (“[T]he burden of low-level arrests is 70% greater among Black civilians than white civilians”); Drew Desilver et al., *10 things we know about race and policing in the U.S.*, Pew Research Center (June 3, 2020), <https://www.pewresearch.org/fact-tank/2020/06/03/10-things-we-know-about-race-and-policing-in-the-u-s/> (“Black adults are about five times as likely as whites to say they’ve been unfairly stopped by police because of their race or ethnicity . . . .”); see also Elizabeth Hinton et al., *An Unjust Burden: The Disparate Treatment of Black Americans in the Criminal Justice System*, Vera (May 2018), <https://www.vera.org/downloads/publications/for-the-record-unjust-burden-racial-disparities.pdf>.

<sup>527</sup> See, e.g., Latoya Hill et al., *Key Facts on Health and Health Care by Race and Ethnicity*, Kaiser Fam. Found. (Jan. 2022), <https://www.kff.org/racial-equity-and-health-policy/report/key-facts-on-health-and-health-care-by-race-and-ethnicity/>; Jesse C. Baumgartner et al., *Racial and Ethnic Inequities in Health Care Coverage and Access, 2013–2019*, Commonwealth Fund (June 9, 2021), <https://www.commonwealthfund.org/publications/issue-briefs/2021/jun/racial-ethnic-inequities-health-care-coverage-access-2013-2019>.

<sup>528</sup> Diana Ellsworth et al., *Racial and ethnic equity in US higher education*, McKinsey & Co. (July 18, 2022), <https://www.mckinsey.com/industries/education/our-insights/racial-and-ethnic-equity-in-us-higher-education>.

<sup>529</sup> See *supra* § II.B.

it is highly likely that the resulting product will replicate and amplify discriminatory outcomes.

**1. Facial recognition technology discriminates on the basis of race and gender; its use generally is an unfair trade practice.**

The Commission should treat the use of facial recognition technology (“FRT”) presumptively as an unfair trade practice in certain contexts and prohibit its use in others, including (1) in public places like streets, parks, and publicly accessible online media; and (2) in settings involving housing, employment, education, credit, insurance, healthcare, places of public accommodation, or other settings involving important life opportunities. Indeed, it should only be allowed in the most controlled and harmless settings, with full knowledge and consent of the participants, and with strict data use limitations isolating the risk.

This is because FRT often is discriminatory on the basis of race and gender. Its use creates a serious risk of misidentification, invasion of privacy, stalking, harassment, government surveillance of protected activities, and other harms. Moreover, it cannot be reasonably avoided: it can be used on images or in public settings or publicly available online images without the consumer ever knowing. The countervailing benefits also do not outweigh the harms—as discussed above, discrimination is an unfair trade practice whose countervailing benefits do not outweigh the harms.<sup>530</sup> And the casual use of FRT for benign purposes, such as to tag ones’ family members in a photo album, does not outweigh the severe risk of abuse by stalkers, domestic abusers, and others who could misuse this spyware technology.

Empirical research demonstrates that FRT presents a significant risk of bias and disparate impact on protected groups by producing inaccurate and skewed outputs. Of all biometric technologies, FRT in particular has received the most criticism for its demonstrated racial and gender bias and its subsequent impact on individuals and communities of color due to its frequent use by law enforcement. Indeed, the data are so alarming that three of the largest purveyors of FRT recently scaled back their operations because of these concerns: IBM and Microsoft both stopped selling FRT products to police departments out of concern that “such technology could be used by the police to violate ‘basic

---

<sup>530</sup> See *supra* § IV.A.3.

human rights and freedoms,”<sup>531</sup> as did Amazon.<sup>532</sup> These concerns have prompted many cities and states to limit the use of FRT by government entities, such as law enforcement, schools, and campus security.<sup>533</sup> However, as long as it is profitable to sell FRT to police departments, schools, and commercial customers, private companies cannot be relied upon to cure these harms through self-regulation.

Several major studies have analyzed commercially available and “state-of-the-art” FRT algorithms and found overwhelming evidence of bias that runs across lines of race, gender, and skin color. One 2018 landmark study, by AI ethics pioneers Joy Buolamwini and Timnit Gebru, “measured the accuracy of three commercial gender classification algorithms” and found that all three systems are more accurate on “male faces than female faces” and “lighter faces than darker faces,” while performing “worst on darker female faces.”<sup>534</sup> The authors noted that despite “darker females [constituting] 21.3% of the [benchmark], they constitute 61.0% to 72.4% of the classification error.”<sup>535</sup> A 2019 study from the National Institute of Standards and Technology (NIST) found similar results when

---

<sup>531</sup> Bobby Allyn, *IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance*, NPR (June 9, 2020), <https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance>; Olivia Solon, *Microsoft won't sell facial recognition to police without federal regulation*, NBC News (June 11, 2020), <https://www.nbcnews.com/tech/internet/microsoft-won-t-sell-facial-recognition-police-without-federal-regulation-n1230286>; see also, Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Its Facial Recognition System*, N.Y. Times (Nov. 5, 2021), <https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html> (describing Facebook’s decision to turn off facial recognition tools but keep the data).

<sup>532</sup> Jeffrey Dastin, *Amazon extends moratorium on police use of facial recognition software*, Reuters (May 18, 2021), <https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/>.

<sup>533</sup> Associated Press, *States Push Back Against Use of Facial Recognition by Police*, U.S. News (May 5, 2021), <https://www.usnews.com/news/politics/articles/2021-05-05/states-push-back-against-use-of-facial-recognition-by-police>. The City of San Francisco prohibited the practice in 2019, followed by California’s statewide three-year moratorium on police use of FRT derived from body cameras. And other states have responded with bans of varying intensity: New York, for example, currently has a two-year moratorium on the use of FRT in schools, while Virginia requires all local law enforcement and campus-based security to get approval from the state legislature before FRT can be utilized. About twenty states are currently considering additional limits and requirements.

<sup>534</sup> Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1, 12 (2018), <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

<sup>535</sup> *Id.* at 10.

it discovered that “a majority of facial-recognition systems exhibit bias,” finding that they “falsely identified African-American and Asian faces 10 times to 100 times more than Caucasian faces.”<sup>536</sup> Research also shows that humans are bad at identifying unfamiliar faces, which can compound discrimination from FRT: humans are likely to make a mistake or rely on an algorithm as authoritative when asked to check and verify the accuracy of the FRT results.<sup>537</sup> One study found that while “many uses of face recognition software have actually increased the need for human processing” to verify results, “[p]rofessional staff who use this technology in their daily work are extremely prone to error, identifying the wrong face from the array on 40% of trials.”<sup>538</sup>

Notably, the founder of one of the most prominent and powerful FRT companies, Clearview AI, reportedly had “deep, longstanding ties to far-right extremists,” some of whom went to work for him.<sup>539</sup> Clearview AI scrapes billions of face photos from publicly available content across the internet—including Facebook, YouTube, and Venmo—to build a massive FRT system that it offers to law enforcement agencies and private businesses nationwide.<sup>540</sup> Reportedly, the technology was developed with backing from an alt-right activist who saw it “as a way to potentially ‘identify every illegal alien in the country’” and who wanted “‘to ID all the illegal immigrants for the deportation squads.’”<sup>541</sup> Over 7,000 employees at over 1,800 public agencies nationwide have used Clearview AI,

---

<sup>536</sup> Patrick Grother et al., *Facial Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, U.S. Dep’t of Com. Nat’l Inst. of Standards & Tech. 14 (Dec. 2019), <https://nvl-pubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

<sup>537</sup> See, e.g., Alice Towler et al., *Can face identification ability be trained? Evidence for two routes to expertise*, in *Forensic face matching: Research and practice* (M. Bindemann ed., 2020), <https://psyarxiv.com/g7qfd/>.

<sup>538</sup> *Id.*

<sup>539</sup> Luke O’Brien, *The Far-Right Helped Create The World’s Most Powerful Facial Recognition Technology*, HuffPost (Apr. 9, 2020), [https://www.huffpost.com/entry/clearview-ai-facial-recognition-alt-right\\_n\\_5e7d028bc5b6cb08a92a5c48](https://www.huffpost.com/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48).

<sup>540</sup> See Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Nov. 2, 2021), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

<sup>541</sup> O’Brien, *supra* note 539.

sometimes without any oversight or even knowledge by their superiors.<sup>542</sup> Clearview AI has raised tens of millions of dollars from investors and continues to be widely used.<sup>543</sup>

FRT has a well-documented history of compounding previously existing racial disparities, particularly when used by or in conjunction with law enforcement.<sup>544</sup> By 2016, approximately half of American adults had records in a law enforcement FRT database.<sup>545</sup> From 2011 to 2017, the New York Police Department claimed it used FRT to make almost 2900 arrests and in 2018 predicted the use of FRT would increase dramatically going forward.<sup>546</sup> “In at least three cases that are publicly known police have relied on erroneous face recognition identifications to make wrongful arrests of Black men,”<sup>547</sup> leading to multiple lawsuits against the police departments that made the arrests.<sup>548</sup> Black Americans are more likely to be stopped, arrested, and incarcerated for minor crimes, and therefore have more mugshots in police databases used for FRT. This creates what some call a “feed-forward loop” making Black Americans disproportionately “subject to future [FRT]

---

<sup>542</sup> Ryan Mac et al., *Surveillance Nation*, BuzzFeed News (Apr. 9, 2021), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition>.

<sup>543</sup> See Kashmir Hill, *Clearview AI raises \$30 million from investors despite legal troubles*, N.Y. Times (Oct. 28, 2021), <https://www.nytimes.com/2021/07/21/technology/clearview-ai-valuation.html>.

<sup>544</sup> Nicol Turner Lee & Caitlin Chin, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*, Brookings (Apr. 12, 2022), <https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>.

<sup>545</sup> Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Priv. & Tech. (Oct. 18, 2016), <https://www.perpetuallineup.org/>.

<sup>546</sup> Clare Garvie, *Garbage in, Garbage Out: Face Recognition on Flawed Data*, Geo. L. Ctr. on Priv. & Tech. (May 16, 2019), <https://www.flawedfacedata.com/>.

<sup>547</sup> New Am.: Open Tech. Inst., *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology* (June 3, 2021), <https://www.newamerica.org/oti/briefs/civil-rights-concerns-regarding-law-enforcement-use-of-face-recognition-technology/>; see also Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (Jan. 6, 2021), <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

<sup>548</sup> See, e.g., Complaint, *Williams v. City of Detroit*, No. 2:21-cv-10827 (E.D. Mich. Apr. 13, 2021), ECF No. 1; Complaint and Demand for Trial By Jury, *Parks v. McCormack*, Case No. PAS-L-003672-20 (N.J. Super. Ct. Law Div. Nov. 25, 2020), <https://int.nyt.com/data/documenttools/new-jersey-facial-recognition-lawsuit-nijeer-parks-v/38ff3e74088a95a9/full.pdf>.

surveillance.”<sup>549</sup> In Detroit in 2016, police installed high-definition cameras throughout the city. While most residents were found in the system, police unevenly distributed the cameras resulting in higher surveillance in predominantly Black areas and little surveillance in predominantly white or Asian areas.<sup>550</sup>

It is difficult to ascertain the full scope of harm caused by law enforcement use of FRT because its use is frequently kept secret. “Across most of the US, neither police nor prosecutors are required to disclose when facial recognition is used to identify a criminal suspect.”<sup>551</sup> Often FRT is not disclosed in a criminal justice proceeding even if it is used during an investigation. Rather, police will use FRT to generate leads on suspects and witnesses and then a human investigator will use that FRT analysis to decide whether two people match.<sup>552</sup> Because even well-trained humans are notoriously bad at facial identification,<sup>553</sup> any flaws in the FRT can substantially influence the human investigator’s determination. At trial, the human will testify that someone matches a person in an image and be cross-examined, but the FRT that provided the initial lead—and potential bias—may not get disclosed to defense counsel or the court. Law enforcement can also use FRT in circumstances that may not lead directly to arrests but nonetheless pose significant risks of abuse—such as surveillance of people experiencing homelessness.<sup>554</sup>

FRT and other biometric technologies developed by commercial vendors and sold to law enforcement agencies are also used to selectively chill protected First Amendment protest activity. Six federal agencies used FRT to identify protestors after George Floyd’s

---

<sup>549</sup> Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Harv. Univ.: Blog: Science Policy (Oct. 24, 2020), <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/?web=1&wdLOR=c495F80EB-3312-4EC4-8695-0AB4D028987B>.

<sup>550</sup> *Id.*; see also Kate Kaye, *Privacy concerns still loom over Detroit’s Project Green Light*, Industry Dive: Smart Cities Dive (Feb. 1, 2021), <https://www.smartcitiesdive.com/news/privacy-concerns-still-loom-over-detroits-project-green-light/594230/>.

<sup>551</sup> Khari Johnson, *The Hidden Role of Facial Recognition Tech in Many Arrests*, Wired (Mar. 7, 2022), <https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/>.

<sup>552</sup> Garvie, *supra* note 546.

<sup>553</sup> See Towler et al., *supra* note 537.

<sup>554</sup> See Joseph Cox, *Tech Firm Offers Cops Facial Recognition to ID Homeless People*, Vice: Motherboard (Feb. 8, 2022), <https://www.vice.com/en/article/wxdp7x/tech-firm-facial-recognition-homeless-people-odin>.

May 2020 murder.<sup>555</sup> In another high-profile incident, the New York Police Department surveilled a racial justice protest, recorded an attendee “speaking loudly into a megaphone,” and attempted to arrest him in his apartment shortly thereafter by sending dozens of officers in riot gear.<sup>556</sup> Baltimore Police used FRT in 2015 during protests over Freddie Gray’s death in police custody.<sup>557</sup> The Baltimore Police’s FRT vendor, Geofeedia, had access to scrape social media data from Facebook, Twitter, and Instagram and feed it to police.<sup>558</sup> This demonstrates how lax privacy practices by commercial actors—even if they do not provide services directly to law enforcement—can exacerbate surveillance of people of color and violation of their rights. Given Black Americans’ overrepresentation in preexisting police databases, law enforcement use of FRT to surveil protestors results in a disparate impact on Black protestors’ likelihood of arrest and in deterring their constitutionally protected activities. While mass surveillance presents risks to everyone, its impact “is conspicuous in the lives of those least empowered to object. Because those communities are over-surveilled, they tend to be over-policed, resulting in inflated arrest rates and increased exposure to incidents of police violence.”<sup>559</sup>

FRT is also a dangerous tool in the hands of stalkers, harassers, vigilantes, and domestic abusers. Companies such as PimEyes offer FRT access to regular consumers, allowing subscribers to input an image of anyone and try to both identify that person and find other images of them on the internet.<sup>560</sup> PimEyes is used to surveil and dox women online: 4chan users found on PimEyes photos “of young girls and women pulled from their social media accounts, their dating-app profiles or ‘creepshots’ stealthily photographed without their consent.”<sup>561</sup> There is currently no national restriction on the

---

<sup>555</sup> Radhamely De Leon, *Six Federal Agencies Used Facial Recognition On George Floyd Protestors*, Vice: Motherboard (June 30, 2021), <https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors>.

<sup>556</sup> Amnesty Int’l, *Ban dangerous facial recognition technology that amplifies racist policing* (Jan. 26, 2021), <https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/>.

<sup>557</sup> Kevin Rector & Alison Knezevich, *Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest*, The Balt. Sun (Oct. 11, 2016), <https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html>.

<sup>558</sup> *Id.*

<sup>559</sup> *Leaders of a Beautiful Struggle*, 2 F.4th at 347 (cleaned up).

<sup>560</sup> Drew Harwell, *This facial recognition website can turn anyone into a cop – or a stalker*, Wash. Post (May 14, 2021), <https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/>.

<sup>561</sup> *Id.*

proliferation of these types of FRT-for-hire services. “It’s not hard to imagine how a technology that turns your smartphone into a personal encyclopedia about anyone you see in a bar or coffee shop could be abused.”<sup>562</sup>

FRT is increasingly being commercially deployed in public venues and schools as well, raising serious concerns of discriminatory access to places of public accommodation and to education. Sports stadiums, arenas, and other large venues are looking to FRT as a new mechanism for tracking admissions and crowds.<sup>563</sup> FRT use by remote proctoring software resulted in students of color having difficulty logging in to take exams.<sup>564</sup> And companies purporting to offer FRT as a solution to school safety disproportionately misidentify Black students and weapons, causing *greater* danger.<sup>565</sup> Other commercial applications for FRT are being developed, such as software specifically designed to determine a person’s race from an image, which has clear risks for abuse.<sup>566</sup>

For these reasons, FRT should not be used in conjunction with access to, eligibility for, or use of important life opportunities such as housing, employment, credit, education, insurance, healthcare, transportation, utility service, and places of public accommodation due to the risk of discrimination, invasion of privacy, and other harms. It likewise should not be used in any public place, such as streets, parks, or publicly accessible online media, because the general public cannot control their exposure and cannot avoid going out in public. Because of the risks of discrimination against people of color, especially women of color, it should be an unfair trade practice for companies to offer FRT services to law

---

<sup>562</sup> Jake Laperruque, *Face Recognition in the Hands of Stalkers, Harassers, and Vigilantes*, Project on Gov’t Oversight (June 10, 2021), <https://www.pogo.org/analysis/2021/06/face-recognition-in-the-hands-of-stalkers-harassers-and-vigilantes>.

<sup>563</sup> See Oliver Thomas, *ASM Global to deploy facial recognition technology across venues*, Conf. & Meetings World (Apr. 22, 2022), <https://www.c-mw.net/asm-global-to-deploy-facial-recognition-technology-across-venues/>; Andrew Cohen, *The New Face of Baseball: Mets to Roll Out Facial Recognition Ticketing at Citi Field*, Sport Techie (Apr. 1, 2022), <https://www.sporttechie.com/the-new-face-of-baseball-mets-to-roll-out-facial-recognition-ticketing-at-citi-field/>; Paul Kapustka, *Easy Entry: Columbus Crew pushes the technology envelope to speed up stadium entry*, Stadium Tech Rep. (Oct. 12, 2021), <https://stadiumtechreport.com/feature/easy-entry-columbus-crew-pushes-the-technology-envelope-to-speed-up-stadium-entry/>.

<sup>564</sup> See Todd Feathers, *Proctorio Is Using Racist Algorithms to Detect Faces*, Vice: Motherboard (Apr. 8, 2021), <https://www.vice.com/en/article/g5qyg3/proctorio-is-using-racist-algorithms-to-detect-faces>; see also Hill, *supra* note 203.

<sup>565</sup> See Feathers, *supra* note 198.

<sup>566</sup> See Parmy Olson, *The Quiet Growth of Race-Detection Software Sparks Concerns Over Bias*, Wall St. J. (Aug. 14, 2020), <https://www.wsj.com/articles/the-quiet-growth-of-race-detection-software-sparks-concerns-over-bias-11597378154>.

enforcement, schools, or administrators of government benefits programs. It should also be an unfair trade practice for companies to offer FRT services to the general public. If allowed at all, FRT should only be permitted in highly restricted settings where (1) there is no risk of deprivation of any benefit or imposition of any cost; (2) the FRT has been proven safe and effective prior to real-world deployment; (3) any data generated by FRT are siloed or ephemeral such that they cannot be used for secondary purposes; and (4) the person on whom FRT is being used—*not* just the user of the FRT—gives informed and explicit consent to use of the technology.

**2. Behavior recognition technologies lack a reliable scientific foundation, carry significant risk of bias and disparate impact, and should be restricted.**

Beyond FRT, some researchers and companies are also attempting to use biometric data to judge or recognize behaviors “objectively.” Although this type of technology is becoming increasingly popular, its reliability is not following suit. Behavioral biometrics technology seeks to identify or make qualitative assessments about individuals based on human behavior. It functions by observing how someone performs a certain action rather than by scrutinizing a discrete biological characteristic.<sup>567</sup> Algorithmic models assess the features of an individual’s behavior to determine uniqueness and patterns.<sup>568</sup> For example, software may analyze an individual’s unique typing rhythm, speed, or cadence, or their speed and step patterns, to create a unique profile to “fingerprint” that individual for future identification. Such technology also may purport to analyze characteristics such as a person’s facial expressions and voice, or to predict an individual’s future actions or their personal traits, dispositions, character, emotions, or other abilities.

Many applications of behavioral biometrics have been labeled “pseudo-science” and “a license to discriminate,” to the extent they are “not rooted in scientific fact.”<sup>569</sup> One study of technology that aimed to discern people’s internal emotional states concluded that “there is insufficient evidence to support” the “common view that humans around the world reliably express and recognize certain emotions in specific configurations of facial

---

<sup>567</sup> Int’l Biometrics & Identity Ass’n, *Behavioral Biometrics* 3 (May 1, 2017), <https://www.ibia.org/download/datasets/3839/Behavioral%20Biometrics%20white%20paper.pdf>.

<sup>568</sup> *Id.* at 4.

<sup>569</sup> Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Wash. Post (Nov. 6, 2019), <https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/>.

movements.”<sup>570</sup> As the study noted, its findings showed conclusively that facial expressions “are not ‘fingerprints’ or diagnostic displays that reliably and specifically signal particular emotional states.”<sup>571</sup>

In this respect, Alan Westin’s prescient writings fifty years ago are still accurate today:

If you make evaluative decisions openly, questioning me directly and justifying your decisions openly, I can fight out publicly your right to judge me in a certain way, and American society will decide our conflicting claims. But if you invoke ‘science’ and ‘expertise’ and evaluate me through personality tests, the issue becomes masked and the public cannot judge the validity and morality of these evaluative decisions. Thus, where such basic issues as political ideology, religion, and race are at stake, the selection process must be objective and public, and I assert my right to privacy to close my emotions, beliefs, and attitudes to the process of job evaluation in a free society.<sup>572</sup>

Indeed, these technologies pose a particularly high risk of discrimination against people with disabilities, such as a person who has suffered partial facial paralysis.

And yet, emotion recognition biometric software is prevalent; the market for it is worth billions.<sup>573</sup> The increased demand for such services is particularly worrisome, as such technologies are increasingly deployed in high-stakes situations, including: a recruiter’s review of a job applicant; “[a] ‘jury’s cultural misunderstanding about what a foreign defendant’s facial expressions mean”; and a “‘smart body’ camera falsely telling a police officer that someone is hostile and full of anger.”<sup>574</sup>

---

<sup>570</sup> Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 Psych. Sci. Pub. Int. 1, 46 (2019), <https://journals.sagepub.com/doi/epub/10.1177/1529100619832930>.

<sup>571</sup> *Id.*

<sup>572</sup> Alan Westin, *Privacy and Freedom* 60–61 (1968).

<sup>573</sup> Jay Stanley, *Experts Say ‘Emotion Recognition’ Lacks Scientific Foundation*, ACLU (July 18, 2019), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/experts-say-emotion-recognition-lacks-scientific>.

<sup>574</sup> *Id.*

Many algorithms used to assess human behavior have been shown to be discriminatory in practice. In 2011, researchers documented the repeated inability of car-based voice recognition systems to accurately detect the speech of women and individuals with thicker accents, which indicates a propensity for discrimination on the basis of sex and national origin.<sup>575</sup> A 2017 study of YouTube’s automatic captioning software found the same, and suggested that the overrepresentation of white, male speakers in the algorithm’s training dataset may be to blame.<sup>576</sup>

Some prominent companies using biometric-based behavioral data are starting to limit the ways biometrics are used to screen job applicants. For example, HireVue announced its decision to stop using facial monitoring in its candidate recruitment software.<sup>577</sup> After auditing its technology, HireVue found little correlation between monitoring facial expressions and candidate success,<sup>578</sup> leading many to worry that the technology would simply “replicate systemic biases that are ingrained in the environment in which they are designed.”<sup>579</sup> The audit suggested HireVue investigate the risk of bias against protected groups and candidates with accents.

The underlying science and studies support the conclusion that the use of behavioral biometrics is discriminatory. The Commission should find that it is an unfair trade practice to use these tools in conjunction with access to, eligibility for, or engagement in important life opportunities such as housing, employment, credit, education, healthcare, insurance, or places of public accommodation.

---

<sup>575</sup> Graeme McMillan, *It’s Not You, It’s It: Voice Recognition Doesn’t Recognize Women*, Time (June 1, 2011) <https://techland.time.com/2011/06/01/its-not-you-its-it-voice-recognition-doesnt-recognize-women/>.

<sup>576</sup> Rachael Tatman, *Gender & Dialect Bias in YouTube’s Automatic Captions*, in *Proceedings of the First Workshop on Ethics in Natural Language Processing* 53–59 (Apr. 4, 2017), <http://www.ethicsinnlp.org/workshop/pdf/EthNLP06.pdf>.

<sup>577</sup> Lindsey Zuloaga, *Industry leadership: New audit results and decision on visual analysis*, HireVue (Jan. 11, 2021), <https://www.hirevue.com/blog/hiring/industry-leadership-new-audit-results-and-decision-on-visual-analysis>. In 2019, a formal complaint was lodged against HireVue with the Federal Trade Commission, alleging the software was “biased, unprovable, and not replicable,” constituting “unfair and deceptive trade practices.” Harwell, *supra* note 569.

<sup>578</sup> Zuloaga, *supra* note 577.

<sup>579</sup> Roy Maurer, *HireVue Discontinues Facial Analysis Screening*, Soc’y Hum. Res. Mgmt. (Feb. 3, 2021), <https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/hirevue-discontinues-facial-analysis-screening.aspx>.

## VII. The FTC should establish robust privacy protections.

To address and prevent unfair and deceptive practices caused by commercial surveillance, the Commission should promulgate regulations to protect data privacy. The following policy recommendations fall into three primary categories: (1) data collection, use, and sharing; (2) consumer rights; and (3) data security. While regulations may need to be more detailed and nuanced than statutes, the Commission should consider legislative proposals and regulatory regimes for guidance on affirmative protections from specific harms that result from otherwise unregulated commercial surveillance practices. In particular, the Commission should look to the proposed American Data Privacy and Protection Act (“ADPPA”),<sup>580</sup> the European Union’s General Data Protection Regulation (“GDPR”),<sup>581</sup> Senator Edward Markey’s Algorithmic Justice and Online Platform Transparency Act bill (“AJOPTA”),<sup>582</sup> the California Consumer Privacy Act (“CCPA”),<sup>583</sup> and the 2019 model privacy bill authored by the Lawyers’ Committee and Free Press.<sup>584</sup>

As a threshold matter, the Commission must recognize that notice and consent is a failed system. In other areas of consumer protection, we do not put the onus on the consumer to protect themselves. We do not allow consumers to consent to having more arsenic in their drinking water or buy a car without air bags and seat belts. Nor do we say “*caveat emptor*” if a consumer does not know how to check that their contractor used proper materials in building their home. Consumers expect a baseline level of safety in the products and services they consume. The same must be true for privacy. There is room for market competition on higher levels of protection (for instance, consumers can buy a car with extra safety features), but there should also be a floor that prohibits unfair practices regardless of knowledge or consent by the consumer. Establishing a floor of

---

<sup>580</sup> H.R. 8152.

<sup>581</sup> Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (“GDPR”), 2016 O.J. (L 119).

<sup>582</sup> Algorithmic Justice and Online Platform Transparency Act, S. 1896, 117th Cong. (2021).

<sup>583</sup> California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (2018).

<sup>584</sup> Free Press Action & Lawyers’ Committee for Civil Rights Under Law, *The Online Civil Rights and Privacy Act of 2019* (2019), [https://www.freepress.net/sites/default/files/2019-03/online\\_civil\\_rights\\_and\\_privacy\\_act\\_of\\_2019.pdf](https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf); see also Gaurav Laroia & David Brody, *Privacy Rights Are Civil Rights. We Need to Protect Them*, Free Press (Mar. 14, 2019), <https://www.freepress.net/blog/privacy-rights-are-civil-rights-we-need-protect-them>.

what data usages are acceptable or unfair—in a permissionless environment—is important for building consumer trust in the ecosystem. If consumers trust that there are guardrails to prevent the abuse of their information, they will be able to use more services more freely, leading to greater use of technology and greater innovation.

### **A. Data collection, use, and sharing**

In response to questions 10, 43–47, and 51, we urge the Commission to establish clear rules regarding the collection, use, processing, retention, and sharing of consumer data. Business practices surrounding data collection—including the vast scope of data gathering, data inferred from aggregation and analysis, and deceptive privacy defaults—demonstrate the harms of the current unregulated market, particularly to communities of color.<sup>585</sup> The current lack of federal regulation of commercial data practices has led to excessive collection of consumer data, deceptive practices surrounding such collection, and unauthorized sharing and use of such data. Since the harms associated with current data practices all “begin[] with extraction,”<sup>586</sup> it is vital to establish strong data minimization policies to regulate the collection, use, sharing, and security of data throughout its life cycle.

#### **1. Data minimization**

The first way to combat harms associated with intrusive data practices is to collect less data. Companies must limit their data processing and sharing to information necessary and proportionate to provide the service requested by the consumer and other enumerated important purposes. In physical as well as online spaces, Black Americans experience “multiple forms of excessive and discriminatory surveillance.”<sup>587</sup> Minimizing the collection, use, and sharing of consumer data is an important step in combatting such discriminatory surveillance practices.

The GDPR provides one model for data minimization.<sup>588</sup> Specifically, the GDPR states that companies should only process personal data that is “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).”<sup>589</sup> The European Data Protection Supervisor (EDPS)—the EU’s

---

<sup>585</sup> See *supra* § III.

<sup>586</sup> Shoshana Zuboff, *You Are the Object of a Secret Extraction Operation*, N.Y. Times (Nov. 12, 2021), <https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html>.

<sup>587</sup> Anita L. Allen, *Dismantling the “Black Opticon”: Privacy, Race Equity, and Online Data-Protection Reform*, Yale L.J.F. 907, 910 (Feb. 20, 2022).

<sup>588</sup> GDPR, 2016 O.J. (L 119) art. 5.

<sup>589</sup> *Id.* art. 5(1)(c).

independent data protection authority established under the GDPR—has defined data minimization as the principle that “a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose.”<sup>590</sup> The ADPPA, currently pending in the House of Representatives, has a similar provision, stating that a “covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to . . . provide or maintain a specific product or service requested by the individual to whom the data pertains.”<sup>591</sup>

Taken together, the GDPR and ADPPA highlight two major aspects of the data minimization principle, the first of which is tied to the company’s *purpose* in processing or sharing data. Current data processing practices lead companies to state their purposes for data collection, use, or sharing broadly (if at all), resulting in excessive and unnecessary data processing. For instance, a survey conducted by the International Data Corporation (IDC) found that companies use only 32 percent of the data that they collect, while the remaining 68 percent is mere noise.<sup>592</sup> The Commission should require companies to clearly articulate a legitimate purpose in collecting, using, or sharing consumers’ data so that their data processing practices are strictly limited in scope to fulfilling that purpose. This articulation should be specific, succinct, and written plainly such that “[e]veryone involved, including data subjects and members of the enterprise, should be able to easily understand the purpose and use of the data.”<sup>593</sup>

Vitaly, this purpose needs to meet clear standards of legitimacy. The ADPPA articulates legitimate uses of data under the heading “permissible purposes.”<sup>594</sup> The Commission should adopt a similar approach and enumerate permissible purposes for collecting, using, or sharing data—and recognize that a purpose may authorize one of those

---

<sup>590</sup>European Data Protection Supervisor, *Data Minimization*, [https://edps.europa.eu/data-protection/data-protection/glossary/d\\_en#:~:text=Data%20minimization,necessary%20to%20fulfil%22that%20purpose](https://edps.europa.eu/data-protection/data-protection/glossary/d_en#:~:text=Data%20minimization,necessary%20to%20fulfil%22that%20purpose) (last visited Nov. 1, 2022).

<sup>591</sup> H.R. 8152 § 101(a); see also *id.* § 102 (establishing stricter data minimization rules for “sensitive” data such as health, location, or financial information).

<sup>592</sup> Cf. Seagate, *Rethink Data: Put More of Your Business Data to Work—From Edge to Cloud* 5 (2020), [https://www.seagate.com/files/www-content/our-story/rethink-data/files/Rethink\\_Data\\_Report\\_2020.pdf](https://www.seagate.com/files/www-content/our-story/rethink-data/files/Rethink_Data_Report_2020.pdf).

<sup>593</sup> Mohammed Khan, *Data Minimization—A Practical Approach*, ISACA (Mar. 29, 2021), <https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach>.

<sup>594</sup> H.R. 8152 § 101(b).

acts but not the others. The Commission should consider the following permissible purposes with regard to non-sensitive personal data:

- To provide or maintain a specific product or service, or to manage or complete transactions, requested by a consumer including associated reasonable routine administrative, accounting, or operational activities;
- To deliver a communication from one individual to another person;
- To authenticate a user, effect product recalls, or fulfill warranties;
- To prevent, detect, protect against, or respond to network security or physical security incidents, and otherwise as needed to protect data security;
- To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity, where such illegal activity can result in harm to an individual;
- To comply with a legal obligation or to pursue or defend against legal claims involving the company;
- To respond to emergencies posing risk of serious injury or death;
- To conduct scientific, historical, or statistical research in the public interest, with appropriate safeguards;

In addition, some purposes may be permissible for processing previously collected data, but may not be a legitimate purpose for collecting new data. Some purposes may be legitimate, or not, for data transfers. For example, transferring personal data in a merger, acquisition, or bankruptcy should only be allowed if each affected individual is given notice and an opportunity to delete their data or withdraw previously given consents. Transferring personal data to a government actor, without either a court order or consent of the individual(s) to whom the information pertain(s), should not be a permissible purpose. And of course a legitimate purpose to take one act does not authorize other secondary uses.

The second aspect of the data minimization principle is related to the *duration* that a consumer's data is retained. Put simply, collected data should not be retained for longer than is necessary to satisfy a legitimate purpose. A failure to erase old or unnecessary data poses significant security risks, as numerous data breaches attest.<sup>595</sup> This is particularly true for communities of color, who are disproportionately affected by "surveillance,

---

<sup>595</sup> See Aaron Drapkin, *Data Breaches That Have Happened in 2022 So Far*, Tech.co (Oct. 26, 2022), <https://tech.co/news/data-breaches-2022-so-far>.

algorithmic bias, and other emerging issues” as well as identity theft and fraud.<sup>596</sup> Thus, the European Commission has clarified data minimization requires that “[d]ata must be stored for the *shortest time possible*” for legitimate business needs, anti-fraud measures, and legal compliance.<sup>597</sup>

The data minimization principle should similarly restrict the sharing of data with data brokers and other third parties. The current lack of regulations surrounding the reuse of data leads to consumer data that “can easily be repurposed to discriminate or over-police in communities of color.”<sup>598</sup> Given that notice and consent regimes are generally ineffective (see Section B(3) below), the Commission should restrict use of data processing and sharing for secondary purposes, even if the data processor could obtain express consent from the consumer. In particular, the Commission should prevent companies that collect data from disclosing non-public personal data to a service provider or third party without contractually requiring that the service provider or third party to meet the same privacy standards as the collecting company.<sup>599</sup>

The Commission should establish stricter data minimization requirements for particularly sensitive personal information.<sup>600</sup> ADPPA Section 102, for instance, states that “a covered entity or service provider may not . . . collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data

---

<sup>596</sup> *Serving Communities of Color*, *supra* note 144, at 3, 7–16, 20.

<sup>597</sup> European Commission, *For How Long Can Data Be Kept and Is It Necessary to Update It?* [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en) (last visited Nov. 1, 2022) (emphasis in original).

<sup>598</sup> Becky Chao et al., *Centering Civil Rights in the Privacy Debate*, New Am.: Open Tech. Inst. 16 (Aug. 2019), <https://www.newamerica.org/oti/reports/centering-civil-rights-privacy-debate/>.

<sup>599</sup> See, e.g., H.R. 8152 § 302.

<sup>600</sup> The ADPPA specifically defines what constitutes “sensitive covered data.” This category includes government-issued identification (such as social security numbers and passports); personal health information (related to both physical and mental health); financial accounts; biometric information; genetic information; precise geolocation data; personal or private communications (including the content of emails, text messages, and voice mail); log-in credentials or security access codes; information related to a person’s sexual preferences or habits; calendar, contact, and address book information; photographs and video information; data related to online activities; information about children; and protected characteristics (including an “individual’s race, color, ethnicity, religion, or union membership”). See *id.* §§ 28(A)(i)–(xvi).

pertains.”<sup>601</sup> The ADPPA further restricts transfers of sensitive data; outside of a few specific situations, sensitive data can only be transferred to a third party with opt-in consent from the consumer.<sup>602</sup>

## 2. Privacy by design and duty of loyalty

The Commission should develop rules for, and require companies to comply with, privacy by design standards. “Privacy by design” ensures that companies are thoughtful in their data practices *before* collecting, using, or sharing information, to ensure compliance with data minimization and data security requirements and prevent harms before they occur. The ADPPA again provides useful models for guidance in addressing this principle, requiring companies to integrate data minimization into their data collection processes. For instance, the ADPPA states that companies should “establish, implement, and maintain reasonable policies, practices, and procedures” that “mitigate privacy risks . . . related to the products and services of the covered entity or the service provider, including in the design, development, and implementation of such products and services.”<sup>603</sup>

The Commission should also establish a “duty of loyalty” on the part of companies collecting, processing, or sharing consumer data that they will not exploit consumer data to cause harm.<sup>604</sup> This duty has been proposed in legislation such as the Consumer Online Privacy Rights Act<sup>605</sup> and the Data Care Act.<sup>606</sup> “Data collectors bound by such a duty of loyalty would be obligated to act in the best interests of the people exposing their data and engaging in online experiences, but only to the extent of their exposure,” and they would be prohibited from “designing digital tools and processing data in a way that conflicts with a trusting party’s best interests.”<sup>607</sup>

---

<sup>601</sup> *Id.* § 102(2).

<sup>602</sup> *See id.* § 102.

<sup>603</sup> *Id.* § 103(a)(3).

<sup>604</sup> *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 Wash. Univ. L. Rev. 961 (2022).

<sup>605</sup> *See* Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 101 (2019).

<sup>606</sup> *See* Data Care Act of 2021, S. 919, 117th Cong. § 3(b)(2) (2021).

<sup>607</sup> Richards & Hartzog, *supra* note 604, at 966.

### 3. Transparency

Transparency—discussed in ANPR questions 83 through 85<sup>608</sup>—plays a key role in consumer protection, the identification of discrimination, and oversight. David Kaye, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has written: “‘Transparency,’ far from being a mantra without meaning, is a powerful tool to challenge the powerful and recover individual agency. . . . [T]ransparency allows users to decide whether to opt into the platforms and how to behave on them if they do.”<sup>609</sup> As such, transparency requirements should be broad, and—as we discuss in response to ANPR questions 89, 90, and 92<sup>610</sup>—they should include full disclosures of a company’s data collection and processing practices using clear and plain language that can be easily understood by consumers. Companies should thus be required to explain their data collection, use, and sharing policies and practices in two ways: (1) exhaustive long form privacy policies that can be scrutinized by experts, researchers, watchdogs, and regulators; and (2) simple short form notices that are easy for any consumer to understand and quickly digest.

The exhaustive privacy policies should accurately and clearly represent the policy choices that a company makes in collecting, processing, retaining, and sharing data. More specifically, these long-form privacy policies should detail at a minimum (1) the types of personal information that the company processes and an explanation of how it obtains such information; (2) the specific permissible purposes for which the company processes each type of data it collects; (3) the names of third parties and service providers with whom the company shares personal information and the specific and legitimate purpose behind each type of disclosure; (4) the duration of data retention for each category of data; (5) a general description of data security practices; (6) a description of how individuals may exercise their rights or otherwise control the company’s processing of their personal information; (7) a description of the method by which the company will notify individuals of material changes to its data policies; and (8) the effective date of the notice.<sup>611</sup> Recognizing the importance of transparency for an open and efficient marketplace, the Commission should narrowly tailor any exceptions from corporate disclosures.

---

<sup>608</sup> ANPR, 87 Fed. Reg. at 51284–85.

<sup>609</sup> David Kaye, *Speech Police: The Global Struggle to Govern the Internet* 121 (2019).

<sup>610</sup> ANPR, 87 Fed. Reg. at 51284–85.

<sup>611</sup> See Free Press Action & Lawyers’ Committee, *The Online Civil Rights and Privacy Act of 2019* (model legislation) 13, <https://www.freepress.net/policy-library/online-civil-rights-and-privacy-act-2019> (last visited Nov. 7, 2022).

A short-form notice specifically designed for consumers should supplement these long-form disclosures. The ADPPA provides a useful model for requirements: the short-form notice must be “concise, clear, conspicuous, and not misleading;” “readily accessible;” “inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person or that involve sensitive covered data;” “a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity;” and “no more than 500 words in length.”<sup>612</sup> The GDPR similarly emphasizes the importance of companies employing clear, concise, and easily understandable language in drafting privacy policies for consumers. Its Recital 58 provides: “The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.”<sup>613</sup> An ideal short form notice fits neatly on one page. The Commission should also develop model short form notices as guidance to businesses.

Privacy notices must also be made available in languages appropriate for a company’s consumer base. The ADPPA stipulates, for instance, that privacy policies should be “made available to the public in each covered language in which the covered entity or service provider—(1) provides a product or service that is subject to the privacy policy; or (2) carries out activities related to such product or service.”<sup>614</sup> It defines “covered language” to mean the ten most used languages in the United States.<sup>615</sup> Privacy notices must also be fully accessible to people with disabilities.

Finally, to promote fair, non-deceptive, and non-predatory data usage, companies that sell or publish advertisements to consumers should maintain and publish a comprehensive “advertisement library.”<sup>616</sup> Advertisement libraries should “contain copies of all advertisements sold or published by the online platform for 2 years following the sale or publishing of each advertisement.”<sup>617</sup> In addition to the content of each advertisement,

---

<sup>612</sup> H.R. 8152 § 202(f).

<sup>613</sup> GDPR, 2016 O.J. (L 119) Recital 58.

<sup>614</sup> H.R. 8152 § 202(c).

<sup>615</sup> *Id.* § 2(10). Capping the number of required languages at a level that covers over 99% the U.S. population is fair even if it does not cover every language a service offers. Wikipedia, for example, provides articles in hundreds of languages and it would be infeasible for it to translate its policies into all of them.

<sup>616</sup> *See, e.g.*, Algorithmic Justice and Online Platform Transparency Act, S. 1896, 117th Cong. § 4(c) (2021).

<sup>617</sup> *Id.* § (c)(5).

each entry in this library should include “all targeting criteria selected by the advertiser, including demographic information,” and “any data the online platform provided to the advertiser regarding to whom it sold or published the advertisement, including demographic information.”<sup>618</sup> These libraries should be easily searchable, accessible, and machine-readable. Making such information publicly accessible would keep companies accountable and help identify potential discrimination or disparate impacts.<sup>619</sup>

## **B. Consumer rights**

This section will address ANPR questions 73 through 82 by outlining the ineffectiveness of consumer consent and the need for other protections.<sup>620</sup> An effective regulatory approach for consumer privacy must confer specific privacy protections and privacy rights. Information on a firm’s privacy practices is of limited use without the corollary ability to act on the information received.

### **1. Consumer’s right to access, correct, delete, and port personal data**

One of the most important privacy rights that consumers should possess is the right to access, correct, delete, and port personal data. These rights are particularly important to combat discrimination: access to data can reveal discrimination, correction can fix inaccurate background reports gatekeeping opportunities,<sup>621</sup> and deletion can frustrate

---

<sup>618</sup> *Id.* § (c)(6)(B), (C).

<sup>619</sup> For instance, referring specifically to the banking industry, the Greenlining Institute has emphasized the importance of data transparency around diversity, inclusion, and equity initiatives: “Data transparency on diversity and inclusion with the Federal Home Loan Banks helps the agency to identify where policy and practice improvements should be made, such as developing incentives and updating outreach methods.” Rawan Elhalaby, *Data Transparency is a Racial Equity Issue: Communities of Color Need Diversity and Inclusion Policies at Banks*, Greenlining Inst. 5 (Feb. 12, 2020), <https://financial-services.house.gov/uploadedfiles/hhrq-116-ba13-wstate-elhalabyr-20200212.pdf>.

<sup>620</sup> ANPR, 87 Fed. Reg. at 51284.

<sup>621</sup> For instance, reports show that “today’s credit reporting bureaus make a tremendous amount of mistakes at the consumers’ expense,” and these mistakes may “[d]isproportionately [i]mpact Black [c]onsumers.” Natalie Campisi, *From Inherent Racial Bias to Incorrect Data—The Problems With Current Credit Scoring Models*, Forbes: Advisor (Feb. 26, 2021), <https://www.forbes.com/advisor/credit-cards/from-inherent-racial-bias-to-incorrect-data-the-problems-with-current-credit-scoring-models/>.

the ability of an abuser to find their target and protect the privacy of people seeking healthcare.<sup>622</sup>

However, at the same time the Commission must consider carefully tailored limits and exceptions to ensure these rights cannot be abused. For example, access rights should not be a tool to unmask whistleblowers or reveal journalistic sources. Deletion rights should not allow an officer to delete a video recording police brutality or allow a politician to hide a detrimental statement.<sup>623</sup>

With regard to correction, consumers should be able to dispute and correct the accuracy or completeness of personal information. Once correction occurs, the entity who collected or holds the data needs to make reasonable efforts to notify all third parties or service providers to which it transferred the data of these data inaccuracies and corrections.<sup>624</sup>

The ability to port one’s data—or transfer personal data between companies—gives consumers control over their personal data. It also can help small businesses build a user base and compete with large corporations, especially small businesses with owners of color.<sup>625</sup> The Open Technology Institute has shown that “data portability and platform interoperability . . . are both critical to ensuring that consumers have control over their data.”<sup>626</sup> If companies “lock down” their data and do not allow consumers to port their data, “tech companies . . . [will] further entrench themselves in the market by making it

---

<sup>622</sup> See, e.g., Bobby Allyn, *Privacy Advocates Fear Google Will Be Used to Prosecute Abortion Seekers*, NPR (July 11, 2022), <https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions>; Tiffany C. Li, *In Post-Roe America, Your Cell Phone Is Now a Reproductive Privacy Risk*, MSNBC (June 26, 2022), <https://www.msnbc.com/opinion/msnbc-opinion/states-abortion-bans-can-weaponize-your-own-data-against-you-n1296591>.

<sup>623</sup> See also Cal. Civ. Code § 1798.105(d) (providing nine exemptions to the right to delete personal data).

<sup>624</sup> See H.R. 8152 § 203(a)(2); see also Cal. Civ. Code § 1798.106.

<sup>625</sup> See, e.g., Bennett Cyphers & Cory Doctorow, *Privacy Without Monopoly: Data Protection and Interoperability*, Elec. Frontier Found. (Feb. 12, 2021), <https://www.eff.org/wp/interoperability-and-privacy>, (explaining that data portability is a vital way of promoting interoperability, which undermines network effects that keep users locked into a conglomerate’s ecosystem and removes barriers to new entrants).

<sup>626</sup> Comments of New America’s Open Technology Institute, *Developing a Privacy Framework*, Nat’l Telecomm. & Info. Admin. Dkt. No. 181101997–8999–02, at 4 (Jan. 14, 2019), [https://www.nist.gov/system/files/documents/2019/02/04/oti\\_eric\\_null.pdf](https://www.nist.gov/system/files/documents/2019/02/04/oti_eric_null.pdf).

harder for consumers to switch services or leverage their own data elsewhere.”<sup>627</sup> Article 20 of the GDPR outlines individuals’ “right to data portability” by stating that individuals “shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.”<sup>628</sup>

Additionally, companies must provide an effective and prompt appeal process when requests to access, correct, delete, or port data are denied. This appeal process should be clearly outlined, easily accessible, and adhere to the transparency principles described above.

## **2. It is unfair to condition service upon a waiver of rights**

The Commission should establish that it is unfair for a company to condition service upon a consumer waiving their right to privacy or waiving other rights (including the right to sue) unless it is impossible for the company to provide service otherwise. Consumers should have the right to opt out of data processing without retaliation or penalty.

The current regulatory vacuum enables companies to coerce consumers into accepting intrusive data collection practices. Consumers “lack bargaining power with companies looking to use their data. Consumers either consent and have access to a service, or they decline and they have no access to that service at all, often without equivalent alternatives.”<sup>629</sup> When consumers are required to assent to take-it-or-leave-it privacy policies, they cannot negotiate terms. Instead, they can simply “decline to use apps or websites—but it’s increasingly hard to participate in the world without them.”<sup>630</sup>

This empty choice particularly harms low-income consumers, who are more likely to be unable to bear the costs associated with the privilege of opting out. Professor Anita Allen has shown, for instance, that “[l]ow-income African Americans may decline privacy protections, such as smartphone encryption, due to prohibitive costs of data-secure

---

<sup>627</sup> *Id.*

<sup>628</sup> GDPR, 2016 O.J. (L 119) art. 20(1).

<sup>629</sup> Claire Park, *How ‘Notice and Consent’ Fails to Protect Our Privacy*, New Am.: Open Tech. Inst. (Mar. 23, 2020), <https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/>.

<sup>630</sup> Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words.*, Wash. Post (May 31, 2022), <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>.

devices and services.”<sup>631</sup> Denials of service or prohibitive cost increases vitiate the concept of consent: “when the choice is between accepting the terms or not gaining access to the service, is that choice even meaningful?”<sup>632</sup>

The CCPA provides useful language for a consumers’ “Right of No Retaliation Following Opt Out.”<sup>633</sup> Section 1798.125 states that a “business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights.”<sup>634</sup> Prohibited practices include:

(A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (C) Providing a different level or quality of goods or services to the consumer. (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.<sup>635</sup>

The Commission should also incorporate the opt-out rights in the ADPPA. First, it provides for the ability to withdraw previously given consents. Section 204 states that a company must “provide an individual with a clear and conspicuous, easy-to-execute means to withdraw any affirmative express consent previously provided by the individual that is as easy to execute by a reasonable individual as the means to provide consent.”<sup>636</sup> The ADPPA also establishes the right to opt-out of data transfers to third parties,<sup>637</sup> which is essential to empowering consumers. A consumer will not know all of the data brokers or other entities that have or could acquire their data, and should not be required to engage in whack-a-mole to protect their privacy. Finally, in the event that the Commission

---

<sup>631</sup> Allen, *supra* note 587, at 916.

<sup>632</sup> Ctr. for Info. Pol’y Leadership, *Are Our Privacy Laws Asking Too Much of Consumers and Too Little of Businesses?* (Dec. 13, 2019), <https://www.informationpolicycentre.com/cipl-blog/are-our-privacy-laws-asking-too-much-of-consumers-and-too-little-of-businesses>.

<sup>633</sup> Cal. Civ. Code § 1798.125.

<sup>634</sup> *Id.* § 1798.125(a)(1).

<sup>635</sup> *Id.* § 1798.125(a)(1)(A)–(D).

<sup>636</sup> H.R. 8152 § 204(a).

<sup>637</sup> *Id.* § 204(b).

does not prohibit targeted advertising as an unfair or deceptive practice, it should at least provide an opt-out right similar to the ADPPA's.<sup>638</sup>

Similarly, the Commission should prohibit forced arbitration agreements as an unfair practice. In 2015, the Consumer Financial Protection Bureau (CFPB) found that, by forcing consumers to sign “arbitration clauses in their contracts that prevent consumers from joining together to sue their bank or financial company for wrongdoing,” companies essentially “sidestep the court system, avoid big refunds, and continue harmful practices.”<sup>639</sup> Public Citizen has similarly shown that “because the private system of forced arbitration benefits companies—and disadvantages consumers and employees—more and more industries are using forced arbitration to evade accountability.”<sup>640</sup> Forced arbitration clauses are not reasonably avoidable by consumers because they are part of contracts of adhesion; consumers have no ability to negotiate them out of terms of service. And there are no countervailing benefits to forced arbitration—to the extent that arbitration is economically efficient and beneficial, parties can always voluntarily choose to arbitrate at the time that a dispute arises.

### **3. Consent can serve a limited role in discrete circumstances.**

In the context of commercial surveillance, consumer consent warrants close scrutiny. Companies purposefully employ “dark patterns”—or the deliberate misleading of users by “obscuring, subverting, or impairing consumer autonomy, decision-making, or choice”—to deceive consumers into giving away their personal data.<sup>641</sup> Examples of dark patterns include online subscriptions and free trials that make it difficult for a user to unsubscribe, deceptively labeled buttons, or graphical elements that direct users’ attention away from certain options on a website.<sup>642</sup>

---

<sup>638</sup> *Id.* § 204(c).

<sup>639</sup> Consumer Fin. Prot. Bureau, *CFPB Issues Rule to Ban Companies From Using Arbitration Clauses to Deny Groups of People Their Day in Court* (July 10, 2017), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-rule-ban-companies-using-arbitration-clauses-deny-groups-people-their-day-court/>.

<sup>640</sup> Pub. Citizen, *Fair Arbitration*, <https://www.citizen.org/article/fair-arbitration/> (last visited Nov. 2, 2022).

<sup>641</sup> FTC, *Bringing Dark Patterns to Light: An FTC Workshop* (Apr. 29, 2021), <https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop>.

<sup>642</sup> Jasmine McNealy, *What Are Dark Patterns? An Online Media Expert Explains*, Nextgov: The Conversation (Aug. 3, 2021), <https://www.nextgov.com/ideas/2021/08/what-are-dark-patterns-online-media-expert-explains/184244/>.

Dark patterns are particularly harmful for consumers of color. For instance, at the Federal Trade Commission’s Workshop on this issue, panelists noted that “greater economic stress, language barriers, and cultural differences all may make non-English speakers and people of color more susceptible to dark patterns and lead to disparate impacts that exacerbate existing racial and socioeconomic disparities.”<sup>643</sup> Yet even in the absence of covert manipulation, “[c]onsent places an immense burden on individuals to protect themselves and understand what is happening with their data. . . . The sheer volume of personal data collected, inferred, used and shared in the digital economy makes this impossible.”<sup>644</sup>

There are, nonetheless, a limited number of discrete circumstances where affirmative, specific, and contextually relevant consent may play a role. In particular, any sharing of sensitive personal information with third parties should require affirmative express consent, obtained on a case-by-case basis, with a specific and conspicuous notice and request explaining why the consent is necessary. Consent should be necessary for data sharing with law enforcement absent a court order.

The opt-in consent governing these specific scenarios should be modeled on the ADPPA’s definition of affirmative express consent.<sup>645</sup> Affirmative express consent entails “an affirmative act by an individual that clearly communicates the individual’s freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity.”<sup>646</sup> This specific request, in turn, should be made “in a clear and conspicuous standalone disclosure” that lists the specific categories of data sought, is written in transparent language, and explains the consumer’s “applicable rights related to consent.”<sup>647</sup> A blanket statement asking consumers to permit their data to be shared “for external processing” does not meet the clear-and specific-purposes standard.<sup>648</sup> In addition, any consent request needs to be made available in

---

<sup>643</sup> *Serving Communities of Color*, *supra* note 144, at 37.

<sup>644</sup> Ctr. for Info. Pol’y Leadership, *supra* note 632.

<sup>645</sup> H.R. 8152 § 2(1).

<sup>646</sup> *Id.* § 2(1)(A).

<sup>647</sup> *Id.* § 2(1)(B)(i)–(vii).

<sup>648</sup> For instance, under the heading, “For External Processing,” Google’s privacy policy provides, in part: “We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help operate our data centers, deliver our products and services, improve our internal business processes, and offer additional support to

languages in which the company routinely provides service and must be made available in a format that is accessible to people with disabilities.

But when relying on consent to address these cases, the Commission must also be extremely careful not to allow a release valve to turn into a loophole. Obtaining consent cannot become a workaround to bypass data minimization rules. If a company could avoid data minimization and other requirements simply by getting user consent, such as through a terms of service agreement when the user initiates service, those requirements would become meaningless. As previously discussed, for a variety of reasons notice and consent does not adequately protect consumers in most circumstances. Only with robust consumer protections will consumers trust the data ecosystem, be able to use services more freely, and rely on those services to innovate.

### C. Data security

In response to ANPR questions 32 and 36, the Commission should establish data security obligations.<sup>649</sup> The policies outlined above would be undermined if malicious actors could breach networks, exploit vulnerabilities in applications, and gain unauthorized access to user data. Accordingly, fair data practices also include implementing data audits, conducting regular security scanning, performing data protection impact assessments, and developing data breach policies and procedures.

Data breaches, identity theft, and fraud are especially harmful to communities of color.<sup>650</sup> Many of these schemes are enabled by companies' lack of adequate data security practices. When a company is negligent in its data security, that increases the risk of breaches of sensitive customer personal information, which can then be used by bad actors to engage in identity theft and other forms of fraud.<sup>651</sup> Moreover, identity theft and fraud are also particularly detrimental to low-income consumers. When a financially secure person has their identity stolen, they often can weather the expense until the situation is resolved. But for people living paycheck to paycheck—especially if they work

---

customers and users.” Google, *Privacy and Terms*, <https://policies.google.com/privacy?hl=en-US#infosharing> (last visited Nov. 2, 2022).

<sup>649</sup> ANPR, 87 Fed. Reg. at 51282.

<sup>650</sup> *Serving Communities of Color*, *supra* note 144, at 20.

<sup>651</sup> See, e.g., Elec. Priv. Info. Ctr., *Equifax Data Breach*, <https://archive.epic.org/privacy/data-breach/equifax/> (last visited Nov. 15, 2022) (discussing how data breaches at major credit bureaus and the Office of Personnel Management led to identity theft, tax fraud, and credit card fraud).

multiple jobs and have little time to spend on hold with customer service departments—a few fraudulent charges can ruin their credit and be devastating.

To protect consumer privacy, companies must secure user data. The GDPR emphasizes the role of businesses in “implement[ing] appropriate technical and organisational measures to ensure a level of security appropriate to the risk” of data storage and processing.<sup>652</sup> With more specificity than the GDPR, the ADPPA offers seven specific data security requirements: (1) assessing vulnerabilities; (2) taking preventative and corrective action; (3) evaluating preventative and corrective action; (4) disposing of unnecessary data; (5) training employees on data security best practices; (6) designating an officer or employee to maintain and implement such practices; and (7) implementing “procedures to detect, respond to, or recover from security incidents, including breaches.”<sup>653</sup> These security requirements should be regularly and independently audited through privacy impact assessments.

### **VIII. The FTC should set distinct rules to protect workers from unfair surveillance practices.**

In question 12, the Commission asks how trade regulation rules should address harms to different kinds of consumers, including workers.<sup>654</sup> The Commission should differentiate workers from consumers when considering how to regulate commercial surveillance.<sup>655</sup> Consumer privacy laws and regulations of general applicability certainly should apply to workers. At the same time, these general laws and regulations do not address unique concerns about workplace surveillance and data-driven technologies, which include impacts on race and gender equity, worker collective action, and health and safety.<sup>656</sup>

Many companies that implement invasive worker surveillance and algorithmic management programs predominantly employ Black, Brown, and other workers of color in positions more likely to be subject to comprehensive and invasive surveillance, such

---

<sup>652</sup> GDPR, 2016 O.J. (L 119) art. 32.

<sup>653</sup> H.R. 8152 § 208(b)(1)–(7).

<sup>654</sup> ANPR, 87 Fed. Reg. at 51281.

<sup>655</sup> The Commission correctly recognized that effective privacy protections must reach “workers of all kinds,” regardless of potential classification or misclassification of a worker as an independent contractor. See *id.* at 51276.

<sup>656</sup> See Annette Bernhardt et al., *Data and Algorithms at Work: The Case for Worker Technology Rights*, UC Berkeley Lab. Ctr. 20 (Nov. 2021), <https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf>.

as in the service sector, warehouses, and the gig economy.<sup>657</sup> Similarly, surveillance systems—such as electronic visit verification imposed on home care workers—disproportionately impact women of color.<sup>658</sup> As with other aspects of commercial surveillance, worker surveillance is more likely to affect communities of color and workers of color are more likely to be negatively affected by flaws or biases in the technologies.

**A. Already-pervasive commercial surveillance of workers has grown more prevalent during the COVID-19 pandemic and rise of the gig economy.**

While worker surveillance is not new, advancements in technology spurred by the COVID-19 pandemic and the gig economy have created more invasive forms of monitoring both inside and outside the workplace.<sup>659</sup>

Companies gather data about their workers in a number of ways. They may purchase it from third parties,<sup>660</sup> directly solicit it from workers,<sup>661</sup> or partner with tech vendors and wellness programs to collect biometric and health data.<sup>662</sup> In addition to these methods of data collection, many companies use electronic monitoring and automated decision-making systems to collect and analyze worker data.

Electronic monitoring entails extensive, and often continuous, monitoring of worker behaviors and actions.<sup>663</sup> While not an exhaustive list, electronic monitoring technologies include: passive sensors, which can capture a wide range of data on worker locations, activities, and interactions with coworkers; systems that log keystrokes and capture screenshots, which enable employers to monitor computer and Internet activity; location

---

<sup>657</sup> *Id.* at 15; see also, e.g., Jodi Kantor et al., *Inside Amazon's Employment Machine*, N.Y. Times (June 15, 2021), <https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html> (noting that Amazon's warehouse workers "are largely people of color"); Irene Tung & Laura Padin, *Silenced About COVID-19 in the Workplace*, Nat'l Emp. L. Project 1 (June 2020), <https://s27147.pcdn.co/wp-content/uploads/Silenced-About-COVID-19-Workplace-Fear-Retaliatio-June-2020.pdf>.

<sup>658</sup> Alexandra Mateescu, *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care*, *Data & Soc'y* 31 (Nov. 2021), [https://datasociety.net/wp-content/uploads/2021/11/EVV\\_REPORT\\_11162021.pdf](https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf).

<sup>659</sup> Bernhardt et al., *supra* note 656, at 1.

<sup>660</sup> *Id.* at 4

<sup>661</sup> *Id.* at 5.

<sup>662</sup> See Ifeoma Ajunwa et al., *Limitless Worker Surveillance*, 105 Cal. L. Rev. 735, 767–69 (2017).

<sup>663</sup> Bernhardt et al., *supra* note 656, at 5.

tracking embedded in vehicles and smartphones, which track workers' movements on and off job sites; and sophisticated computer vision, which is used to analyze video captured by workplace cameras in real time.<sup>664</sup>

Automated decision-making tools, including the use of algorithms, are used in a variety of ways in the workplace, from retention or promotion decisions to instructions for delivery drivers.<sup>665</sup> Common uses include human resource analytics, such as hiring, performance evaluation, and on-the-job training;<sup>666</sup> productivity management, such as scheduling, coordination, and direction of worker activities;<sup>667</sup> and task automation.

### 1. Workplace data-driven technologies in practice.

Data-driven technologies are used extensively in the workplace in a range of ways. The examples used here are only illustrative and are not comprehensive.

- **Remote monitoring.** Many industries use remote monitoring technologies. In call centers, tools like Teleperformance TP Observer use webcams with a computer vision system that monitors workers at their computers and attempts to detect if they are following company policies in real-time.<sup>668</sup> In retail, XBRi Loss Prevention System monitors cashiers and provides a list of workers with a high likelihood for suspicious transactions.<sup>669</sup>
- **Performance monitoring.** Cogito provides technology systems that monitor, record, and analyze interactions between call center employees and customers and can provide real-time behavioral guidance to workers about pace and demeanor.<sup>670</sup> Drivers

---

<sup>664</sup> *Id.* Computer vision is a field of artificial intelligence that allows computers to identify objects or derive other meaning from video footage and other visual inputs. IBM, *What Is Computer Vision?*, <https://www.ibm.com/topics/computer-vision> (last visited Oct. 8, 2022).

<sup>665</sup> Bernhardt et al., *supra* note 656, at 5.

<sup>666</sup> *Id.* at 6.

<sup>667</sup> *Id.*

<sup>668</sup> *Id.*; Wilneida Negrón, *Little Tech Is Coming for Workers*, Coworker.org 61 (Nov. 2021), <https://home.coworker.org/wp-content/uploads/2021/11/Little-Tech-Is-Coming-for-Workers.pdf>.

<sup>669</sup> Negrón, *supra* note 668, at 61.

<sup>670</sup> Tom Simonite, *This Call May Be Monitored for Tone and Emotion*, Wired (Mar. 19, 2018), <https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/>; Cogito, *Augmented Intelligence in the Contact Center: The Why, What, and How* 9,

are also monitored by apps like Mentor, which track and measure behaviors such as harsh braking, speeding, making cell phone calls and sending texts, seatbelt use, and driving in reverse.<sup>671</sup>

- **Productivity monitoring.** Software vendors like RedOwl and Humanyze collect keystrokes and searches, as well as expression in email and physical movements.<sup>672</sup> WorkSmart takes screenshots of workers' screens and combines that information with other data to provide a productivity measurement.<sup>673</sup> Teramind measures focus by collecting data on how often a worker switches apps.<sup>674</sup>
- **Location monitoring.** The construction industry is increasingly adopting geofencing technologies to automatically clock workers in and out and track travel time between job sites.<sup>675</sup> Nurses in Florida wear geolocation tags to track the time they spend with patients and how efficiently they are moving through the hospital.<sup>676</sup> Some companies use apps like Xora StreetSmart that allow employers to see the location of every mobile worker on a Google Map.<sup>677</sup>

---

<https://cogitocorp.com/wp-content/uploads/2020/12/WP-4Ws-Augmented-Intelligence-r3.1.pdf> (last visited Nov. 15, 2022).

<sup>671</sup> Annie Palmer, *Amazon Uses an App Called Mentor to Track and Discipline Delivery Drivers*, CNBC (Feb. 12, 2021), <https://www.cnbc.com/2021/02/12/amazon-mentor-app-tracks-and-disciplines-delivery-drivers.html>; eDriving, *Mentor DSP by eDriving Driver Guide*, <https://www.edriving.com/mentor-dsp-by-edriving-driver-guide/> (last visited Oct. 8, 2022).

<sup>672</sup> Sam Adler-Bell & Michelle Miller, *The Datafication of Employment*, The Century Foundation 13 (Dec. 19, 2018), <https://production-tcf.imgix.net/app/uploads/2018/12/03160631/the-datafication-of-employment.pdf>.

<sup>673</sup> Joelle Gamble, *The Inequalities of Workplace Surveillance*, The Nation (June 3, 2019), <https://www.thenation.com/article/archive/worker-surveillance-big-data/>.

<sup>674</sup> Olivia Solon, *Big Brother Isn't Just Watching: Workplace Surveillance Can Track Your Every Move*, The Guardian (Nov. 6, 2017), <https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology>.

<sup>675</sup> Bernhardt et al., *supra* note 656, at 13.

<sup>676</sup> David F. Carr, *Florida Hospital Tracks Nurses Footsteps, Work Patterns*, Info. Wk. (Mar. 17, 2014), <https://www.informationweek.com/analytics/florida-hospital-tracks-nurses-footsteps-work-patterns>.

<sup>677</sup> James Vincent, *Woman Fired After Disabling Work App That Tracked Her Movements 24/7*, The Verge (May 13, 2015), <https://www.theverge.com/2015/5/13/8597081/worker-gps-fired-myrna-arias-xora>.

- **Safety monitoring.** Workplaces like construction sites use computer vision to prevent worksite accidents in real-time.<sup>678</sup>
- **Task direction algorithms.** Hotel management software can delegate tasks to hotel staff based on room status or workers' proximity and workload.<sup>679</sup> UPS's ORION (On-Road Integrated Optimization and Navigation) creates deliverers' routes and updates them in real time as customers' preferences change.<sup>680</sup>
- **Scheduling algorithms.** A number of companies use proprietary software for scheduling.<sup>681</sup> Percolata sets productivity scores and creates schedules by monitoring and measuring in-store customer traffic and worker activities.<sup>682</sup>
- **Biometric collection and use.** The use of biometrics is also becoming more common. Amazon recently required its truck drivers to consent to the use of biometric data, including facial recognition, within their trucks to confirm identity and connect to driver accounts.<sup>683</sup> Some contract attorneys have also been required to use facial recognition software while working remotely.<sup>684</sup> As discussed above, these technologies frequently fail to correctly identify people of color, especially Black women.<sup>685</sup>

## 2. Workplace surveillance has become more ubiquitous since the COVID-19 pandemic.

While it is difficult to know how many companies use monitoring technologies, a 2018 Gartner survey of 239 large corporations found that more than half were using “non-traditional monitoring techniques” such as “analyzing the text of emails and social media-messages, scrutinizing who’s meeting with whom, gathering biometric data and

<sup>678</sup> Bernhardt et al., *supra* note 656, at 13.

<sup>679</sup> *Id.* at 12; Alexandra Mateescu & Aiha Nguyen, *Explainer: Algorithmic Management in the Workplace*, Data & Soc’y 9 (Feb. 2019), [https://datasociety.net/wp-content/uploads/2019/02/DS\\_Algorithmic\\_Management\\_Explainer.pdf](https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf).

<sup>680</sup> Mateescu & Nguyen, *supra* note 679, at 7.

<sup>681</sup> *Id.* at 9.

<sup>682</sup> Bernhardt et al., *supra* note 656, at 9.

<sup>683</sup> Lauren Kaori Gurley, *Amazon Delivery Drivers Forced to Sign ‘Biometric Consent’ Form or Lose Job*, Vice: Motherboard (Mar. 23, 2021), <https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job>.

<sup>684</sup> Drew Harwell, *Contract Lawyers Face a Growing Invasion of Surveillance Programs That Monitor Their Work*, Wash. Post (Nov. 11, 2021), <https://www.washingtonpost.com/technology/2021/11/11/lawyer-facial-recognition-monitoring/>.

<sup>685</sup> See *supra* § VI.C.

understanding how employees are utilizing their workspace.”<sup>686</sup> A contributor at Gartner projected that this number would jump to nearly 80% by the end of 2020, and that was before we knew the COVID-19 pandemic was looming.<sup>687</sup>

The pandemic accelerated the digitization of the workplace.<sup>688</sup> The increase in data-driven technologies included cameras that ensured workers were complying with social distancing requirements and time-clock apps with facial recognition features.<sup>689</sup> A 2021 study of over 550 “Little Tech” worker management products found that artificial intelligence (“AI”) and platform-based business models started to enter the emerging “care economy.”<sup>690</sup>

The pandemic also expanded the potential data points that can be collected from workers. In the wake of the pandemic, companies deployed and normalized technologies

---

<sup>686</sup> Brian Kropp, *The Future of Employee Monitoring*, Gartner (May 3, 2019), <https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring>.

<sup>687</sup> *Id.*

<sup>688</sup> Bernhardt et al., *supra* note 656, at 14.

<sup>689</sup> Daniel A. Hanley & Sally Hubbard, *Eyes Everywhere: Amazon’s Surveillance Infrastructure and Revitalizing Worker Power*, Open Mkts. Inst. 8 (Sept. 2020), [https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cfea23958d79eae1ab23/1598881772432/Amazon\\_Report\\_Final.pdf](https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cfea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf); see also Bernhardt et al., *supra* note 656, at 14; Daniel A. Hanley, *Eyes Everywhere: Amazon’s Surveillance Infrastructure and Revitalizing Worker Power – An Update*, Open Mkts. Inst. (Sept. 2021), <https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/614ca2f0d599c17dd163cbf6/1632412400295/Hanley+-+UPDATE+to+Amazon%27s+Surveillance+Infrastructure-FINAL.pdf>.

<sup>690</sup> Negrón, *supra* note 668, at 34. This report was based on Coworker.org’s “Bossware and Employment Tech” database, which compiled “more than 550 labor-focused technology products that are changing our relationship to work.” Coworker.org, *Bossware and Employment Tech Database* (Nov. 17, 2021), <https://home.coworker.org/worktech>. Coworker.org is a nonprofit organization that “deploy[s] digital tools, data, and strategies in service of helping people improve their work lives.” Coworker.org, *About Us* (last visited Oct. 10, 2022), <https://home.coworker.org/about-us/>. In contrast to Big Tech companies like Amazon, Apple, Facebook, Google, and Microsoft, Little Tech is “the unregulated marketplace of tech products that are collecting and aggregating data about workers at almost every step of the labor process.” Negrón, *supra* note 668, at 6. The “care economy” refers to public and private services for childcare, early childhood education, elder care, and disability and long-term care. *Id.* at 34 n.100.

that collected sensitive medical data as they sought to minimize the spread of the virus.<sup>691</sup> Investments for companies seeking to capture “personal medical and behavioral data in the workplace, such as information on emotions, stress levels, anxiety, mood, and more” increased.<sup>692</sup>

Because the COVID-19 pandemic created remote working environments for many people, the desire to track workers away from the office increased substantially.<sup>693</sup> Employers often required white-collar workers to download software that tracked and measured their productivity throughout the day, sometimes by keeping computer cameras and microphones on.<sup>694</sup>

Sales for two companies’ surveillance software spiked 500% and 600% between March and June of 2020.<sup>695</sup> Of the 550 products cataloged by Coworker.org, 31% emerged between 2020 and 2021.<sup>696</sup> And journalists documented nearly 500 new COVID-related iOS apps between March and October 2020, further empowering employers’ capability to mine and purchase sensitive medical data.<sup>697</sup>

---

<sup>691</sup> Negrón, *supra* note 668, at 32; see also Aiha Nguyen, *The Constant Boss: Work Under Digital Surveillance*, *Data & Soc’y* 3 (May 2021), [https://datasociety.net/wp-content/uploads/2021/05/The\\_Constant\\_Boss.pdf](https://datasociety.net/wp-content/uploads/2021/05/The_Constant_Boss.pdf).

<sup>692</sup> Negrón, *supra* note 668, at 32.

<sup>693</sup> Hanley & Hubbard, *supra* note 689, at 2.

<sup>694</sup> Nguyen, *supra* note 691, at 5.

<sup>695</sup> Hanley & Hubbard, *supra* note 689, at 6; Adam Isaak, *Employee Tracking Is Increasingly Widespread, and It Could Be Doing More Harm Than Good*, CNBC (June 17, 2020), <https://www.cnbc.com/2020/06/17/employee-surveillance-software-is-seeing-a-spike-as-workers-stay-home.html> (“Prodoscore, said it has seen a 600% increase in interest from prospective customers since the pandemic hit. Another, TransparentBusiness, said it has seen a 500% spike in users month to month.”); see also Bennett Cyphers & Karen Gullo, *Inside the Invasive, Secretive “Bossware” Tracking Workers*, EFF (June 30, 2020), <https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers> (“Awareness Technologies, which owns InterGuard, claimed to have grown its customer base by over 300% in just the first few weeks after the outbreak.”).

<sup>696</sup> Negrón, *supra* note 668, at 24.

<sup>697</sup> *Id.* (citing Jonathan Albright, *The Pandemic App Ecosystem: Investigating 493 Covid-Related iOS Apps across 98 Countries*, Medium (Oct. 28, 2020), <https://d1gi.medium.com/the-pandemic-app-ecosystem-investigating-493-covid-related-ios-apps-across-98-countries-cdca305b99da>).

### 3. The gig economy has created new opportunities for worker surveillance.

Corporations that operate digital labor platforms such as Uber, Lyft, and TaskRabbit pioneered many of the techniques of management algorithms, which input data collected via worker surveillance into algorithms that assign, optimize, and evaluate workers.<sup>698</sup> Since gig companies seek to manage large pools of workers with variable schedules and locations, management algorithms are most visible through gig work. For gig workers, the entire work experience is mediated by algorithms that influence them toward specific behaviors regarding work times, customer engagement, and productivity.<sup>699</sup>

Gig work has become more prevalent in the last decade.<sup>700</sup> In fact, one in three U.S. workers relies on gig work to sustain their livelihood.<sup>701</sup> The proliferation of gig labor companies and productivity-enhancing algorithms is “deepening and accelerating the datafication of employment”<sup>702</sup> and extracting more work, data, efficiency, and productivity from workers.<sup>703</sup>

---

<sup>698</sup> Matt Scherer, *Warning: Bossware May Be Hazardous to Your Health*, Ctr. for Democracy & Tech. 8 (July 24, 2021), <https://cdt.org/wp-content/uploads/2021/07/2021-07-29-Warning-Bossware-May-Be-Hazardous-To-Your-Health-Final.pdf>; see also Cyphers & Gullo, *supra* note 695.

<sup>699</sup> Adler-Bell & Miller, *supra* note 672, at 11; see also Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers’ Buttons*, N.Y. Times (Apr. 2, 2017), <https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html>.

<sup>700</sup> See ADP Rsch. Inst., *ADP Research Institute Report Reveals the Gig Workforce is Filling a Void in the Tight Labor Market* (Feb. 4, 2020), <https://www.adpri.org/media/adp-research-institute-report-reveals-the-gig-workforce-is-filling-a-void-in-the-tight-labor-market/>.

<sup>701</sup> Rani Molla, *More Americans Are Taking Jobs Without Employer Benefits Like Health Care or Paid Vacation*, Vox (Sep. 3, 2021), <https://www.vox.com/recode/22651953/americans-gig-independent-workers-benefits-vacation-health-care-inequality>.

<sup>702</sup> Negrón, *supra* note 668, at 7; see also Adler-Bell & Miller, *supra* note 672.

<sup>703</sup> Negrón, *supra* note 668, at 7; see also Scherer, *supra* note 698, at 8.

**B. Worker surveillance that undermines workers' rights is an unfair or deceptive trade practice.**

**1. Workers face unique and substantial harms from commercial surveillance.**

Workplace surveillance and certain data-driven practices cause substantial injury to workers. They have disrupted workers' right to organize, threatened worker safety, caused discrimination harms, resulted in wage theft, and facilitated deceptive and unfair earnings claims, among other substantial harms. Below we explain some of these harms more fully.

**a. Commercial surveillance preempts and disrupts workers' protected right to organize and bargain collectively.**

The National Labor Relations Act (NLRA) gives employees the rights to “self-organization, to form, join, or assist labor organizations, to bargain collectively . . . and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.”<sup>704</sup> Interfering with these rights is an unfair labor practice.<sup>705</sup> There are growing concerns, including from the National Labor Relations Board, that surveillance can be used to chill efforts by workers to exercise their protected right to unionize or take actions to change workplace conditions.<sup>706</sup> Indeed, surveillance of workers' activities, movements, locations, communications, and social media accounts—including predictive heat maps and detailed tracking software—put workers' unionization and collective action rights at risk.

For instance, in 2012, after hearing about the possibility of a Black Friday strike, Walmart hired an intelligence-gathering service from Lockheed Martin to monitor the social media of activists to determine which stores were most at risk.<sup>707</sup> Last year, the fast

---

<sup>704</sup> 29 U.S.C. § 157.

<sup>705</sup> *Id.* § 158(a).

<sup>706</sup> Nat'l Lab. Rels. Bd. Off. Pub. Affs., *NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices* (Oct. 31, 2022), <https://www.nlr.gov/news-outreach/news-story/nlr-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and>; Nguyen, *supra* note 691, at 22–23; Bernhardt et al., *supra* note 656, at 16.

<sup>707</sup> Susan Berfield, *How Walmart Keeps an Eye on Its Massive Workforce*, Bloomberg Businessweek (Nov. 24, 2015), <https://www.bloomberg.com/features/2015-walmart-union-surveillance/>. Walmart was not alone in surveilling employees. See e.g., Lauren Kaori Gurley, *Secret Amazon Reports Expose the Company's Surveillance of Labor and Environmental Groups*, Vice Motherboard (Nov. 23, 2020),

food labor activist campaign “Fight for \$15” filed a charge with the National Labor Relations Board (NLRB) against McDonald’s after an investigation revealed a secret intelligence program that monitored workers’ activities through data collection software and social media monitoring.<sup>708</sup> Whole Foods and Amazon also keep tabs on stores likely to unionize through “heat maps” based on scores derived from survey data and other factors such as date of last pay raise.<sup>709</sup> In addition, Amazon has used its geoSPatial Operating Console to analyze and visualize public data on unions.<sup>710</sup>

**b. Worker surveillance mentally and physically harms workers.**

The Occupational Safety and Health Act (OSH Act) requires employers to maintain a safe and healthful workplace. The General Duty Clause of the OSH Act requires employers to keep workplaces free from any recognized hazards that cause or are likely to cause death or serious physical harm to employees.<sup>711</sup> The Occupational Safety and Health Administration (OSHA) further regulates safety at places of employment by issuing

---

<https://www.vice.com/en/article/5dp3yn/amazon-leaked-reports-expose-spying-warehouse-workers-labor-union-environmental-groups-social-movements>; Thuy Ong, *Amazon Patents Wristbands That Track Warehouse Employees’ Hands in Real Time*, Verge (Feb. 1, 2018), <https://www.theverge.com/2018/2/1/16958918/amazon-patents-trackable-wristband-warehouse-employees>; James Vincent, *Amazon Is Reportedly Surveilling Its Flex Delivery Drivers in Private Facebook Groups*, Verge (Sept. 2, 2020), <https://www.theverge.com/2020/9/2/21418057/amazon-surveilling-flex-delivery-drivers-facebook-groups-subreddits-strikes-protests>.

<sup>708</sup> Lorenzo Franceschi-Bicchierai & Lauren Kaori Gurley, *‘Fight for \$15’ Files Charges Against McDonald’s for Illegally Spying on Workers*, Vice: Motherboard (Apr. 1, 202), <https://www.vice.com/en/article/k7a4gy/fight-for-dollar15-files-charges-against-mcdonalds-for-illegally-spying-on-workers>; Lorenzo Franceschi-Bicchierai & Lauren Kaori Gurley, *McDonald’s Secretive Intel Team Spies on ‘Fight for \$15’ Workers, Internal Documents Show*, Vice: Motherboard (Feb. 24, 2021), <https://www.vice.com/en/article/pkdkz9/mcdonalds-secretive-intel-team-spies-on-fight-for-15-workers>.

<sup>709</sup> Sarah Kessler, *Companies Are Using Employee Survey Data to Predict – and Squash – Union Organizing*, OneZero (July 30, 2020), <https://onezero.medium.com/companies-are-using-employee-survey-data-to-predict-and-squash-union-organizing-a7e28a8c2158>; Hayley Peterson, *Amazon-Owned Whole Foods Is Quietly Tracking Its Employees with a Heat Map Tool That Ranks Which Stores Are Most at Risk of Unionizing*, Bus. Insider (Apr. 20, 2020), <https://www.businessinsider.nl/whole-foods-tracks-unionization-risk-with-heat-map-2020-1/>; Jason Del Rey & Shirin Ghaffary, *Leaked: Confidential Amazon Memo Reveals New Software to Track Unions*, Recode (Oct. 6, 2020), <https://www.vox.com/recode/2020/10/6/21502639/amazon-union-busting-tracking-memo-spoc>.

<sup>710</sup> Negrón, *supra* note 668, at 61; Del Rey & Ghaffary, *supra* note 709.

<sup>711</sup> 29 U.S.C. § 654(a)(1).

more specific standards.<sup>712</sup> Digital surveillance and automated decision-making systems designed to squeeze productivity and efficiency out of workers result in dangerous and unhealthy working conditions, evidenced by frequent and serious worker injuries and psychological distress.

For example, Amazon subjects its workers to “time off task” (“TOT”) tracking and strict termination measures, which leads to dangerous and unhealthy working conditions and worker injury.<sup>713</sup> Amazon’s TOT tracking calculates the time a worker spends not completing the task assigned by the worker’s item scanner. Workers may be automatically terminated for falling behind the required work rate too many times.<sup>714</sup> Afraid of automatic termination, workers at Amazon may feel compelled to work through pain and injuries incurred on the job, as time spent attending to injuries may not be excluded from the TOT tracker.<sup>715</sup> In fact, the rate of severe injuries at some Amazon warehouses is five times the industry average.<sup>716</sup>

Gaps in the OSH Act and OSHA’s enforcement authority necessitate action by the Commission to protect worker privacy and safety. OSHA does not enforce its standards in home or remote offices,<sup>717</sup> leaving those who work outside the traditional workplace defenseless against injuries caused by surveillance. Further, OSHA has no specific standard regarding increasingly prevalent injuries due to repetitive motion, fatigue, pace of work, or threats to mental health.<sup>718</sup> Finally, OSHA’s enforcement authority and resources are constrained. And OSHA has limited authority to obtain injunctions, forcing it to rely on issuing fines to deter employers from violating its standards.<sup>719</sup>

---

<sup>712</sup> *Id.* § 654(a)(1)-(2).

<sup>713</sup> See Hanley & Hubbard, *supra* note 689, at 10–12.

<sup>714</sup> *Id.* at 10.

<sup>715</sup> *Id.* at 11; see also Michael Sainato, *Accidents at Amazon: Workers Left to Suffer After Warehouse Injuries*, The Guardian (July 30, 2018), <https://www.theguardian.com/technology/2018/jul/30/accidents-at-amazon-workers-left-to-suffer-after-warehouse-injuries>.

<sup>716</sup> Reveal, *Find Out What Injuries Are Like at the Amazon Warehouse That Handled Your Packages* (Nov. 25, 2019), <https://revealnews.org/article/find-out-what-injuries-are-like-at-the-amazon-warehouse-that-handled-your-packages/>.

<sup>717</sup> Scherer, *supra* note 698, at 33–34.

<sup>718</sup> *Id.* at 18.

<sup>719</sup> *Id.* at 17.

**c. Discriminatory technological practices cause substantial and unique harms to workers.**

Title VII of the Civil Rights Act of 1964 prohibits employers from discriminating on the basis of race, color, religion, sex, or national origin. However, evidence of persistent discrimination, such as disproportionate employment of Black and Brown workers in low-wage jobs, remains widespread.<sup>720</sup> As mentioned above, worker surveillance and algorithmic management programs are more likely to adversely affect workers of color, particularly women of color.

Surveillance technology and data collection are deployed in many service-sector industries and in the gig economy, which disproportionately employ people of color. Two-thirds of the front-line warehouse workforce are people of color,<sup>721</sup> and 95% of domestic workers are “women, foreign-born persons, [and/or] persons of color[.]”<sup>722</sup> Moreover, workers in restaurants and other food services are disproportionately people of color: 47.7% of workers in this sectors are people of color.<sup>723</sup> Gig workers are also disproportionately people of color; 30% of Latinx adults, 20% of Black adults, and 19% of Asian adults have engaged in gig work, compared to only 12% of white adults.<sup>724</sup>

Black and Brown workers are disproportionately harmed by algorithmic decision-making in the workplace. Data-driven systems that monitor individuals for suspicious behavior can be influenced by racial and ethnic profiling.<sup>725</sup> For example, some post-hiring

---

<sup>720</sup> See generally Yeshimabeit Milner & Amy Traub, *Data Capitalism and Algorithmic Racism*, Demos, at 10 (May 17, 2021), <https://www.demos.org/research/data-capitalism-and-algorithmic-racism>.

<sup>721</sup> Beth Gutelius & Nik Theodore, *The Future of Warehouse Work*, UC Berkeley Lab. Ctr., at 6 (Oct. 22, 2019), <https://laborcenter.berkeley.edu/future-of-warehouse-work/>.

<sup>722</sup> Kyle Boyd, *The Color of Help*, Ctr. for Am. Progress (June 17, 2011), <https://www.americanprogress.org/issues/race/news/2011/06/17/9783/the-color-of-help/>.

<sup>723</sup> U.S. Bureau of Lab. Stat., *Labor Force Statistics from the Current Population Survey: Household Data Annual Averages, 18. Employed Persons by Detailed Industry, Sex, Race, and Hispanic or Latino Ethnicity* (Jan. 20, 2022), <https://www.bls.gov/cps/cpsaat18.htm>.

<sup>724</sup> *Serving Communities of Color*, *supra* note 144, at 19 (citing U.S. Bureau of Labor Statistics, *Electronically Mediated Work: New Questions in the Contingent Worker Supplement*, U.S. Dep’t of Lab. tbls. 3 & 4 (Sept. 2018), <https://www.bls.gov/opub/mlr/2018/article/electronically-mediated-work-new-questions-in-the-contingent-worker-supplement.htm>).

<sup>725</sup> See Nguyen, *supra* note 691, at 21.

monitoring tools can notify an employer if a worker has been arrested, even if the activity was not recorded in court records.<sup>726</sup> Due to the disproportionate rates at which people of color are arrested because of racial profiling, these tools accelerate systemic racism in the workplace.<sup>727</sup> A study of worker management products determined that “most lack the necessary safeguards and have not conducted sufficient due diligence and impact assessment to ensure products do not discriminate on the basis of protected classes under federal law.”<sup>728</sup>

Finally, some electronic monitoring has strayed outside of the workplace, such as technology that scans social media and app activity or accesses GPS location data when a worker is not on the clock.<sup>729</sup> This type of intrusive surveillance can uncover sensitive and private information about workers, such as their religion, sexual orientation, gender identity, or disability that have no bearing on their jobs.<sup>730</sup>

## **2. Workers have no practical means to avoid harms from workplace surveillance.**

For the overwhelming majority of workers, commercial surveillance and harmful data-driven technologies are not reasonably avoidable. Workers suffer from an inherent employer-worker power imbalance that can strip consent of any real meaning and leave workers without knowledge or control of workplace technologies.

Power imbalances between employers and workers nullify the notion that workers can give consent to surveillance. For most workers in the United States, the workplace holds an inherent power asymmetry, which denies them a say in the policies and decisions that affect their day-to-day lives.<sup>731</sup> Workers cannot easily raise objections to environments with undesired or dangerous technology policies when they rely on employment to meet basic survival needs.<sup>732</sup> The increasing information asymmetry caused by data-driven technologies only worsens this power imbalance. Data collection and surveillance

---

<sup>726</sup> Business Wire, *HireRight Debuts Suite of Advanced Post-Hire Employee Monitoring Solutions* (May 18, 2020), <https://www.business-wire.com/news/home/20200518005121/en/HireRight-Debuts-Suite-of-Advanced-Post-Hire-Employee-Monitoring-Solutions>.

<sup>727</sup> Nguyen, *supra* note 691, at 21–22.

<sup>728</sup> Negrón, *supra* note 668, at 7.

<sup>729</sup> Bernhardt et al., *supra* note 656, at 17.

<sup>730</sup> *Id.*

<sup>731</sup> *Id.* at 19.

<sup>732</sup> See, e.g., Gurley, *supra* note 683.

allow employers to know more about their workers and their activities than workers know about their employers and their employer's activities. Likewise, productivity monitoring allows an employer to wield excessive power over workers.<sup>733</sup> Layoff and bonus decisions tied to algorithmically generated performance metrics can exacerbate power imbalances in the workplace.<sup>734</sup>

Workers often have no knowledge, input, or control over workplace technologies, and no recourse to contest errors or rights violations. Software for tracking workers, sometimes called "bossware," can generally be deployed in two ways: first, as an app that is visible to, and sometimes controlled by, a worker; second, as a secret background process that workers cannot see.<sup>735</sup> Of the surveillance technology firms with public-facing marketing materials, most give employers the option to install their software either way.<sup>736</sup> Since this software is explicitly designed to evade detection, there is no reliable way for workers to know they are being surveilled.<sup>737</sup> Employers are not required to notify workers about electronic monitoring or algorithms upon which they are basing decisions,<sup>738</sup> and workers do not have an express right to know what data is being gathered on them or whether it is being sold or shared with others. Nor do they have the right to review or correct that data.<sup>739</sup> In addition, without regulation or oversight, workers are especially vulnerable to untested or faulty systems.<sup>740</sup> Disclosure could alleviate these harms.

### **3. Putative benefits of worker surveillance used to violate workers' rights do not outweigh the harms.**

The Commission should find that alleged countervailing benefits of worker surveillance do not outweigh the substantial injury of losing essential and statutorily-guaranteed protections. In fact, many forms of worker surveillance and related data-driven technologies incentivize practices that decrease efficiency in the workplace.

---

<sup>733</sup> Cyphers & Gullo, *supra* note 695.

<sup>734</sup> See Hanley & Hubbard, *supra* note 689, at 12.

<sup>735</sup> Cyphers & Gullo, *supra* note 695.

<sup>736</sup> *Id.*

<sup>737</sup> *Id.*

<sup>738</sup> Bernhardt et al., *supra* note 656, at 18.

<sup>739</sup> *Id.*

<sup>740</sup> *Id.* at 2, 18.

While public policy benefits may not serve as the primary basis for an unfairness determination,<sup>741</sup> they are persuasive factors to consider and the worker surveillance practices catalogued above implicate essential worker protections. These protections include the right to organize, the right to safe work conditions, and the right to be free from discrimination on the basis of protected characteristics. While these protections may come at a cost to employers, cost-savings from denying or undermining these protections are not the types of “benefits to consumers or to competition” that the Commission’s unfairness tests countenances.<sup>742</sup> Congress has already decided, through legislation protecting those rights, that the benefits of preventing harms to workers outweigh the costs.

Rather than increasing the efficiency of an employer’s workforce, constant monitoring incentivizes workers to reallocate time spent working to time spent appeasing workplace surveillance technologies. Workers feel forced to jiggle their mouse or type for the sake of typing, stifling their creativity.<sup>743</sup> Important work like thinking critically and tending to patients is discounted or disregarded entirely.<sup>744</sup> For example, hospice chaplains are asked to accrue “productivity points” based on actions they take like whether they visit the dying (one point), participate in a funeral (one and three-quarters points), or call grieving relatives (one-quarter point)—shifting whom the chaplains see and the depth of their relationships, with one chaplain describing making “spiritual care drive-bys” to rack up points.<sup>745</sup> And a financial executive subjected to extensive monitoring software found that her paychecks were low because the system did not account for offline work, like reading, doing math problems on paper, or mentoring junior colleagues.<sup>746</sup> Surveillance technologies may register workers as being productive, even where they are less efficient, reducing the marginal benefit of these technologies to employers.

### **C. Guidance for rules to limit the harms of worker surveillance.**

Employees have a reasonable expectation that employers will follow the law and will not use commercial surveillance in a manner that violates their statutorily-protected

---

<sup>741</sup> 15 U.S.C. § 45(n).

<sup>742</sup> *Id.*

<sup>743</sup> Cyphers & Gullo, *supra* note 695.

<sup>744</sup> See Jodi Kantor & Arya Sundaram, *The Rise of Worker Productivity Score*, N.Y. Times (Aug. 14, 2022), <https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html>.

<sup>745</sup> *Id.*

<sup>746</sup> *Id.*

rights. Thus, when commercial surveillance practices are used to violate existing labor and employment rights, they are unfair or deceptive practices.

At the same time, existing employment and labor rights inadequately protect workers from the substantial harms caused by many commercial surveillance and automated management practices. One reason is generally only workers who are deemed “employees” under the various labor and employment statutes are entitled to their protections. Yet, as illustrated below, commercial surveillance and technology are increasingly facilitating harms to workers whether they are engaged as employees or independent contractors.<sup>747</sup>

In addition, worker protection laws are difficult to enforce when violations are committed through the use of commercial surveillance. These laws fail to provide workers with the right to access information about the use of such technologies and fail to require preventative measures such as impact assessments and audits. In addition, employment laws fail to take into consideration the harms to customers of businesses that deploy such unfair or deceptive practices. And extant worker protection laws do not regulate third parties such as vendors who provide harmful technologies that are used to facilitate unfair and deceptive trade practices affecting workers.

Thus, we urge the Commission to prevent unfairness to or deception of workers from data-driven technologies in the workplace. Below, we identify areas where Commission action is appropriate and areas where the Commission should work with other competent agencies in crafting specific regulations.

- **Anti-discrimination.** As discussed above, the use of automated decision-making tools, surveillance, or any other data-driven technology—including the use of data and algorithmic outputs—to engage in discrimination based on protected characteristics should be deemed an unfair trade practice. And where a worker is reasonably misled as to the firm’s representation, practice, or omission about the discriminatory use of such technology, the practice should be deemed deceptive.<sup>748</sup>
- **Organizing and Bargaining.** Unions should have the right to bargain over workplace surveillance, and surveillance tools should not be used to interfere with the exercise of employees’ rights to engage in protected, concerted activity, to organize, or any

---

<sup>747</sup> See Press Release, FTC, *Amazon To Pay \$61.7 Million to Settle FTC Charges It Withheld Some Customer Tips from Amazon Flex Drivers* (Feb. 2, 2021), <https://www.ftc.gov/news-events/press-releases/2021/02/amazon-pay-617-million-settle-ftc-charges-it-withheld-some>.

<sup>748</sup> See *supra* § IV.

other rights under the NLRA. Companies should also be prohibited from using data processing practices, surveillance, and predictive technologies that interfere protected rights to speak out and take collective action in the workplace. The Commission should restrict technologies used to identify or predict organizing activity or purported “predisposition” to organizing; data processing for the purpose of retaliating against workers for organizing, whistleblowing, or engaging in collective action; and the use of any technologies that have a tendency to interfere with workers’ rights under section 7 of the NLRA.

- **Disclosure.** The Commission should require companies to provide clear, accessible information about their surveillance and data-driven technologies that affect workers, whether used in or outside the workplace. Workers should have the right to know which technologies are being used to surveil them, the data the technologies collect, and the impact of electronic monitoring on their work. Without this data, workers are unable to determine whether any violations of their rights may have occurred.
- **Worker Data.** The Commission should require companies to follow reasonable data minimization practices similar to the recommendations above.<sup>749</sup> The worker-employer relationship is fundamentally different from the consumer-merchant relationship, so the rules will likely need to be different to account for this. Within the scope of employment, employers may have justified reasons to collect and use certain data that would not be justified for a merchant. Appropriate data minimization rules for employers include requiring companies to clearly and succinctly articulate their purposes for collecting, using, and sharing categories of workers’ data, limiting data collection to what is reasonably necessary and proportionate for those articulated purposes, and adopting extra protections for particularly sensitive data. Moreover, companies must use responsible data security practices. Finally, the rules should recognize that if an employer seeks to surveil a worker *outside* the scope of employment, on matters unrelated to their work, then the employer should have to meet the regular rules that apply in the consumer-merchant relationship.
- **Use of Unsafe Electronic Monitoring and Algorithms.** Companies should not use high-risk technologies—such as facial recognition and other biometrics—or algorithmic systems that harm worker safety, such as those that contribute toward unsafe work intensification.
- **Impact Assessments.** The Commission should require vendors and users to conduct impact assessments of surveillance practices and automated decision-making systems if there is a reasonable chance they will result in discriminatory impacts or impair

---

<sup>749</sup> See *supra* § VII.

the mental and physical safety of workers.<sup>750</sup> Workers should be consulted in conducting those assessments and given access to their results.

- **Interagency Collaboration.** The Commission shares an interest to protect workers with other government agencies. The Commission’s recent memoranda of understanding with the National Labor Relations Board to share information and training regarding areas of common regulatory interest in the “gig economy” provides a roadmap for successful collaboration on other issues.<sup>751</sup> OSHA, the Equal Employment Opportunity Commission, Department of Labor, Department of Justice, Consumer Financial Protection Bureau, and other agencies with issue- or sector-specific expertise can be valuable partners in both identifying unfair trade practices in the workplace and in developing appropriate regulatory responses to mitigate the harmful impacts of those practices.

#### **IX. The First Amendment does not block FTC action to protect civil rights and privacy.**

In response to question 63 of the ANPR,<sup>752</sup> the Commission can promulgate and enforce rules concerning the personalization of services and delivery of targeted advertisements without running afoul of the First Amendment. First, these issues concern unprotected conduct, not speech, and therefore do not implicate the First Amendment. And even if regulation of this conduct imposes incidental burdens on speech, regulation is permissible so long as it promotes a substantial governmental interest that would be achieved less efficiently absent the regulation. Second, to the extent the data practices at issue are considered speech, they concern commercial speech subject to lesser or no protection under the First Amendment. Third, even if the regulations ultimately implicate protected speech, they will survive strict scrutiny so long as they are narrowly tailored to serve compelling interests such as preventing fraud, discrimination, and voter intimidation.

---

<sup>750</sup> See *supra* § VI.B.4.

<sup>751</sup> See Memorandum of Understanding Between the Federal Trade Commission (FTC) and the National Labor Relations Board Regarding Information Sharing, Cross-Agency Training, and Outreach in Areas of Common Regulatory Interest (July 19, 2022), <https://www.nlr.gov/sites/default/files/attachments/pages/node-7857/ftcnlrb-mou-71922.pdf>.

<sup>752</sup> ANPR, 87 Fed. Reg. at 51284.

**A. Algorithmic systems, including targeted advertising, involve unprotected conduct and otherwise merely incidentally affect speech.**

The freedom of speech ranks “among our most cherished liberties,”<sup>753</sup> but its protections do not extend to all conduct.<sup>754</sup> Indeed, it only protects conduct that is “inherently expressive.”<sup>755</sup> Thus, laws “directed at the communicative nature of conduct” or “at speech itself,” such as laws prohibiting the burning of the American flag, undergo strict scrutiny.<sup>756</sup> But when laws are not directed at speech itself—in other words, when “the governmental interest is unrelated to the suppression of free expression”—then a “relatively lenient standard” applies.<sup>757</sup> This is so even where there is an “incidental burden” on speech.<sup>758</sup>

The standard for such content neutral laws considers whether a regulation “promotes a substantial government interest that would be achieved less effectively absent the regulation.”<sup>759</sup> Although the regulation may not be “substantially broader than necessary to achieve the government’s interest,” it need not be the “least intrusive means of achieving the desired end.”<sup>760</sup>

In this context, the Supreme Court has differentiated between the regulation of speech, which merits strict scrutiny, and the regulation of speech’s amplification, which is content neutral and need only promote a substantial government interest that would be achieved less effectively absent the regulation.<sup>761</sup> In *Ward v. Rock Against Racism*, the Court considered the constitutionality of a city’s sound amplification guidelines, which required performers at a city venue to use sound-amplification equipment and a sound technician provided by the city.<sup>762</sup> The justifications for the guideline were “the city’s desire to control noise levels at bandshell events” and to “ensur[e] the quality of sound at Bandshell

---

<sup>753</sup> *Pittsburgh Press*, 413 U.S. at 381.

<sup>754</sup> See *United States v. O’Brien*, 391 U.S. 367, 376 (1968).

<sup>755</sup> *Rumsfeld v. F. for Acad. & Institutional Rts., Inc.*, 547 U.S. 47, 66 (2006).

<sup>756</sup> *Texas v. Johnson*, 491 U.S. 397, 406–07 (1989).

<sup>757</sup> *Id.* at 407.

<sup>758</sup> *Rumsfeld*, 547 U.S. at 67.

<sup>759</sup> *Id.* (citation omitted).

<sup>760</sup> *Ward v. Rock Against Racism*, 491 U.S. 781, 797, 799 (1989) (quotation omitted).

<sup>761</sup> See *Rumsfeld*, 547 U.S. at 67.

<sup>762</sup> *Ward*, 491 U.S. at 784, 791.

events.”<sup>763</sup> The Court found that the guideline was a constitutional content-neutral policy that had “nothing to do with content.”<sup>764</sup>

Like in *Ward*, where the Court held that amplification of speech could be subjected to reasonable time, place, and manner restrictions to consider the effect on the surrounding community, so too can the Commission regulate amplification of online content and other platform architectures. Regulation of algorithmic systems including automated decision-making systems, personalized recommendations, and targeted advertising has “nothing to do with content,” and thus the First Amendment does not require scrutiny of its regulation. Personalized recommendations are conduct no different than shopping with the assistance of a sales associate or tailoring a suit for a better fit. Similarly, while recommended content (including advertisements) may be speech, the mechanisms that deliver the content are not. Rather, the delivery mechanisms are infrastructure used to deliver content in the same way as telephone and cable television wires, the radio spectrum, and the sound amplification system in *Ward*. Thus, these services concern conduct, not speech, and therefore fall outside the First Amendment’s ambit.

Even if regulation of this conduct imposes incidental burdens on speech, its regulation is permissible so long as it promotes a substantial governmental interest that would be achieved less efficiently absent the regulation. One such interest is combating discrimination. Indeed, laws targeting “the act of discrimination” pass muster under the First Amendment even though they might cause an incidental burden on speech.<sup>765</sup> For example, “a ban on race-based hiring may require employers to remove ‘White Applicants Only’ signs.”<sup>766</sup> Or the enforcement of a public accommodation statute that forbids discrimination on basis of sex may cause “some incidental abridgment” of protected speech by requiring that women be admitted into an organization.<sup>767</sup> But “[w]here the government does not target conduct on the basis of its expressive content, acts are not shielded from regulation merely because they express a discriminatory idea or philosophy.”<sup>768</sup>

---

<sup>763</sup> *Id.* at 792.

<sup>764</sup> *Id.* (quotation omitted).

<sup>765</sup> *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos.*, 515 U.S. 557, 572 (1995); see also *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 567 (2011) (“[T]he First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech.”).

<sup>766</sup> *Sorrell*, 564 U.S. at 567.

<sup>767</sup> *U.S. Jaycees*, 468 U.S. at 628.

<sup>768</sup> *R.A.V. v. City of St. Paul, Minn.*, 505 U.S. 377, 390 (1992).

**B. If speech is implicated, it is commercial speech subject to lesser protection under the First Amendment.**

The Constitution “accords a lesser protection to commercial speech than to other constitutionally guaranteed expression.”<sup>769</sup> Commercial speech is “expression related solely to the economic interests of the speaker and its audience.”<sup>770</sup> A four-part analysis determines whether a regulation concerning commercial speech is valid:

At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.<sup>771</sup>

As noted in *Pittsburgh Press*, this analysis disposes of First Amendment protection for commercial activity that “itself is illegal.”<sup>772</sup>

Assuming personalization services and delivery of advertisements concern speech, these issues implicate only commercial speech: they relate solely to the economic interests of companies and their users and customers. Any regulations aimed at preventing deceptive practices and discrimination would concern misleading and unlawful commercial speech that would not be afforded any First Amendment protection.<sup>773</sup> Any regulations that target other speech would withstand scrutiny so long as they advance the governmental interest asserted and are not more extensive than necessary to serve that interest.<sup>774</sup>

---

<sup>769</sup> *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of N.Y.*, 447 U.S. 557, 563 (1980).

<sup>770</sup> *Id.* at 561 (citations omitted).

<sup>771</sup> *Id.* at 566.

<sup>772</sup> *Pittsburgh Press*, 413 U.S. at 389.

<sup>773</sup> See *In re R. M. J.*, 455 U.S. 191, 202 (1982) (inherently deceptive speech); *Pittsburgh Press*, 413 U.S. at 389 (discrimination).

<sup>774</sup> See *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566.

The fact that ad delivery systems interact with ad content does not change the analysis—it is still commercial speech. In *Pittsburgh Press*, the Court dealt with a city ordinance prohibiting newspapers from carrying advertisements in sex-designated columns except where the employer or advertiser was free to make hiring or employment referral decisions on the basis of sex.<sup>775</sup> After holding that the advertisements themselves were commercial advertisements, the Court found that the newspaper’s “editorial judgment” concerning where to place the advertisements did not warrant First Amendment protection.<sup>776</sup> Indeed, placing a want ad in a “Jobs–Male Interest” column “conveys essentially the same message as an overtly discriminatory want ad, [and] is in practical effect an integrated commercial statement.”<sup>777</sup>

Ad delivery systems function in the same way as the newspaper’s editorial judgment in *Pittsburgh Press*. The ads are commercial speech. The delivery systems—determinations on how those ads should be delivered—are not entitled to any additional protections. Indeed, when those delivery systems discriminate by considering protected characteristics and by resulting in the disparate delivery of advertisements to individuals based on protected characteristics, it has the same effect as the overtly discriminatory want ads in *Pittsburgh Press*.

**C. Even if non-commercial speech is implicated, preventing fraud, discrimination, and voter intimidation are compelling government interests.**

The Commission can assert at least three compelling interests to sustain regulations even if they implicate protected speech. First, there is “[n]o doubt” that “the government’s interest in preventing fraud is generally a compelling government interest.”<sup>778</sup>

Second, the government has a compelling interest in “eradicating discrimination” against its citizens, particularly discrimination against Black people and members of other historically marginalized communities.<sup>779</sup> The Court has reiterated this “compelling interest” in a variety of situations, including in upholding public accommodations statutes that

---

<sup>775</sup> *Pittsburgh Press*, 413 U.S. at 378.

<sup>776</sup> *Id.* at 385–88.

<sup>777</sup> *Id.* at 387–88.

<sup>778</sup> *Nat’l Cap. Presbytery v. Mayorkas*, 567 F. Supp. 3d 230, 246 (D.D.C. 2021) (collecting cases).

<sup>779</sup> *U.S. Jaycees*, 468 U.S. at 623.

require equal treatment based on sex,<sup>780</sup> upholding the IRS’s policy of requiring that tax-exempt private schools have racially nondiscriminatory policies,<sup>781</sup> and in holding there must be “equal opportunity to participate in the workforce without regard to race.”<sup>782</sup>

Third, it is axiomatic that the right to vote is “preservative of all rights,”<sup>783</sup> and the federal government indisputably has a compelling interest in “protect[ing] voters from confusion and undue influence” and “preserv[ing] the integrity of its election process.”<sup>784</sup> In *Burson v. Freeman*, the Supreme Court held that ballot privacy laws survived a strict scrutiny challenge when they restricted electioneering near polling places—political speech at the core of the First Amendment—because they prevented voter intimidation.<sup>785</sup> Laws prohibiting voter suppression, such as the Voting Rights Act, have been held to be narrowly tailored to advance compelling government interests even if they result in content-based restrictions on speech.<sup>786</sup>

Thus, even if the FTC promulgates regulations that undergo strict scrutiny, they will survive the analysis so long as they are narrowly tailored to combat fraud, discrimination, voter intimidation, or other compelling government interests.

\* \* \*

For these reasons, the First Amendment does not prevent the FTC from issuing regulations to prevent discrimination and protect privacy in the personalization of services and delivery of advertisements.

## **X. Conclusion**

For the foregoing reasons, the Lawyers’ Committee urges the Commission to use its authority under Section 5 of the FTC Act to prohibit discrimination as an unfair and deceptive practice, to consequently prohibit any commercial surveillance practices that result in discrimination—including targeted advertising, unbounded use of automated

---

<sup>780</sup> *Id.* at 628; *Bd. of Directors of Rotary Int’l v. Rotary Club of Duarte*, 481 U.S. 537, 549 (1987); see also *Heart of Atlanta Motel*, 379 U.S. at 260.

<sup>781</sup> *Bob Jones Univ. v. United States*, 461 U.S. 574, 604 (1983).

<sup>782</sup> See, e.g., *Burwell*, 573 U.S. at 733.

<sup>783</sup> *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886); accord *Reynolds v. Sims*, 377 U.S. 533, 562 (1964).

<sup>784</sup> *Burson v. Freeman*, 504 U.S. 191, 199 (1992) (plurality).

<sup>785</sup> *Id.* at 200–08 (discussing the history of ballot privacy regimes).

<sup>786</sup> See *Nat’l Coal. on Black Civic Participation v. Wohl*, 498 F. Supp. 3d at 486 n. 29.

decision-making systems, and biometrics technologies such as facial recognition—and promulgate regulations to protect the privacy of individuals against intrusive commercial surveillance practices.

**Appendix A: ANPR Questions Addressed in Lawyers' Committee's Comments**

Question	Sections Addressing Questions
3-6	III
10	IV VII (including VII.A)
11	VI (including VI.A.2)
12	III IV VI (including VI.A.2) VIII
24-25	II
29	II III
30	III
32, 36	VII (including VII.C)
37-38	VI (including VI.C)
39	II IV VI (including VI.A.4)
40	IV VI (including VI.A.4)
41	VI (including VI.A.4)
43-47	VII (including VII.A)
50	II III
51	VII (including VII.A)
53	III VI (including VI.B.3)
55	III VI (including VI.B.1)
56	VI (including VI.B.4)
57	III
60	IV
61	VI (including VI.B.4)
62	V VI
63	IX
65	III VI (including VI.B.1)
66	III VI (including VI.B.1)
67	IV (including IV.C & IV.D) VI (including VI.B.4)
68	II

	III IV (including IV.D)
69	III V
70	V
71	IV V
72	V
73–82	VII (including VII.B)
83–85, 89–90, 92	VII (including VII.A.3)