New York Office
40 Rector Street, 5th Floor
New York, NY 10006
T 212.965.2200
F 212.226.7592

www.naacpldf.org

Washington, D.C. Office
700 14th Street, NW, Suite 600
Washington, D.C. 20005
T 202.682.1300
F 202.682.1312

November 21, 2022

Submitted electronically via Regulations.gov
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue
NW, Suite CC–5610 (Annex B)
Washington, DC 20580

RE: Commercial Surveillance ANPR, R111004

To Whom It May Concern,

On behalf of the NAACP Legal Defense and Educational Fund, Inc. (LDF), we submit the following comments in response to the Federal Trade Commission's Advanced Notice of Proposed Rulemaking on commercial surveillance and data privacy. Automated decision-making systems (ADSs) now permeate every area of our lives, from hiring and other aspects of employment, to identifying and securing housing, to accessing government services and supports. Yet there are instances when these systems are not only ineffective but also reproduce or exacerbate inequities, bias, and discrimination. ADSs can exhibit algorithmic bias, creating unfair disadvantages for people of color and other protected classes by preventing them from learning about opportunities, denying them access to opportunities, or requiring them to pay more for the same services. Commercially-developed ADSs and other technologies—some of which may themselves exhibit algorithmic bias, misrepresent their effectiveness, and/or rely on large amounts of sensitive, personal data—can also be deployed by law enforcement in ways that disproportionately harm communities of color, endangering their liberty and physical safety, and risking a range of collateral consequences.

While some existing civil rights laws may prohibit algorithmic bias against protected classes, these laws are insufficient to protect against algorithmic bias, deceptively marketed ADSs, or the discriminatory deployment of ADSs and other technologies by law enforcement. As discussed below, the lack of transparency about the development and deployment of ADSs makes it more difficult for harmed individuals to seek redress, and the absence of comprehensive regulation of these systems often permits widespread harm before the companies that develop these technologies or the entities that deploy them identify and mitigate their risks, if they do at all, or consult with

affected communities. We urge the FTC to use its existing regulatory authority to protect consumers from algorithmic bias, including bias in products where the end user is a government entity. It should also use its authority to prevent the harms caused by commercially-developed technologies, particularly those that leverage large amounts of sensitive data, that are used by law enforcement to discriminate against communities of color.

Founded in 1940 by Thurgood Marshall, LDF is the nation's oldest civil rights law organization.[1] LDF was launched at a time when America's aspirations for equality and due process of law were stifled by widespread state-sponsored racial inequality. For more than 80 years, LDF has relied on the Constitution and federal and state civil rights laws to pursue equality and justice for Black Americans and other people of color. LDF's mission has always been transformative: to achieve racial justice, equality, and an inclusive society.

Since its inception, LDF has worked to increase fairness and equal opportunity for Black Americans. Some of Thurgood Marshall's early victories in the Supreme Court came in *Shelley v. Kramer*, 334 U.S. 1 (1948), and *McGhee v. Sipes*, 334 U.S. 1 (1948), which held that the state enforcement of racially restrictive covenants violated the Equal Protection Clause. In the decades since those victories, LDF's litigation, policy advocacy, organizing, and public education programs have sought to ensure the fundamental rights of all people to quality education, economic opportunity, the right to vote and fully participate in democracy, and the right to a fair and just judicial system. LDF has continued to challenge public and private policies and practices that deny Black Americans housing, employment, health care, and other opportunities,[2] and has fought to address unconstitutional and racially discriminatory law enforcement conduct.[3]

Throughout this comment, we will use the term "ADS" to encompass a variety of automated tools that analyze data using algorithms to make decisions or recommendations. At its most basic, an algorithm is a set of instructions to accomplish a task.[4] Artificial intelligence (AI) is a highly

[1] LDF has been fully separate from the National Association for the Advancement of Colored People (NAACP) since 1957.

[2] *E.g. Griggs v. Duke Power Co.,* 401 U.S. 424 (1971); *Phillips v. Martin Marietta Corp.*, 400 U.S. 542 (1971); *Albemarle Paper Co. v. Moody*, 422 U.S. 405 (1975); *Pullman-Standard v. Swint*, 456 U.S. 273 (1982); *Anderson v. City of Bessemer City*, 470 U.S. 564 (1985); and *Lewis v. City of Chi.*, 560 U.S. 205 (2010). *Linton v. Comm'r of Health & Env't*, 65 F.3d 508 (6th Cir. 1995) (preservation of Medicaid-certified hospital and nursing home beds to prevent eviction of patients in favor of admitting more remunerative private-pay individuals); *Bryan v. Koch*, 627 F.2d 612 (2d Cir. 1980) (challenge to closure of municipal hospital serving inner-city residents); *Simkins v. Moses H. Cone Mem'l Hosp*., 323 F.2d 959 (4th Cir. 1963) (admission of African-American physician to hospital staff); *Mussington v. St. Luke's-Roosevelt Hosp. Ctr.*, 824 F. Supp. 427 (S.D.N.Y. 1993) (relocation of services from inner-city branch of merged hospital entity); *Rackley v. Bd. of Trs. of Orangeburg Reg'l Hosp*., 238 F. Supp. 512 (E.D.S.C. 1965) (desegregation of hospital wards); Consent Decree, *Terry v. Methodist Hosp. of Gary*, Nos. H-76-373, H-77-154 (N.D. Ind. June 8, 1979) (planned relocation of urban hospital services from inner-city community).

[3] *Tennessee v. Garner*, 471 U.S. 1 (1985) (a seminal case that held, for the first time, that police officers cannot shoot "fleeing felons" who do not pose a threat to officers or members of the public); *see also Davis, et al. v. City of New York, et al*., 902 F. Supp. 2d 405 (S.D.N.Y. 2012).

[4] *See, e.g.,* Stephen F. DeAngelis, *Artificial Intelligence: How Algorithms Make Systems Smart,* WIRED, https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/ (last visited Nov. 4, 2022).

contested term that generally refers to computer technologies that use algorithms to approximate human capabilities, such as learning, decision-making, image recognition, and language processing.[5] For example, Netflix uses AI to generate recommendations based on your viewing history.[6] Machine learning is a subset of AI that uses large data sets to train models to mimic capabilities such as prediction and recognition.[7] When we refer to ADSs, we are including AI and systems that use machine learning, as well as other types of algorithms.

I. Algorithmic Bias Can Arise in a Variety of ADSs Due to Model Design, Incomplete or Unrepresentative Data, and Systemic Inequality Due to Past Discrimination.

ADSs can lead to unequal outcomes based on race or other characteristics—or algorithmic bias—for several reasons:

- *Model Design:* An ADS can be designed to allow companies to exclude or deny access to consumers on the basis of particular characteristics, such as race.[8] An ADS can also be explicitly designed to rely on variables that are known proxies for those characteristics.[9] For example, an ADS that uses zip codes to decide to whom to provide services and on what terms could lead to discrimination against Black and other customers of color due to the history of redlining and ongoing residential segregation.[10] These choices are often embedded in the variables that designers choose to include in their model. For example, as discussed in more detail below, the lending platform Upstart chose to include borrowers' educational data, including their SAT scores, in its model.[11] This decision resulted in borrowers of color receiving substantially worse loan terms due to racial disparities in SAT scores resulting from the well-known bias embedded in the tests.[12]

---

[5] *See, e.g.,* Darrell M. West, *What is Artificial Intelligence*, BROOKINGS INST. (Oct. 14, 2018), https://www.brookings.edu/research/what-is-artificial-intelligence/.
[6] DeAngelis, *supra* note 4.
[7] Sara Brown, *Machine learning, explained,* MIT SLOAN SCHOOL OF MANAGEMENT (Apr. 21, 2021), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained.
[8] *U.S. Dep't of Hous. & Urban Dev. v. Facebook,* FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.
[9] Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data,* 8 YALE J.L. & TECH. 148, 182 (2016), hurley_18yjolt136_jz_proofedits_final_7aug16_clean_0.pdf; *see also* Compl. ¶ 67, *United States v. Meta Platforms, Inc.,* No. 22-cv-05187 (SDNY Jun. 21, 2022), https://www.justice.gov/opa/press-release/file/1514026/download.
[10] Hurley & Adebayo, *supra* note 9, at 182; *see* TOM SHAPIRO ET AL., LDF THURGOOD MARSHALL INST. & INST. ON ASSETS AND SOC. POL'Y AT BRANDEIS UNIV., THE BLACK-WHITE RACIAL WEALTH GAP 7-9 (2019), https://tminstituteldf.org/wp-content/uploads/2019/11/FINAL-RWG-Brief-v1.pdf; Bruce Mitchell & Juan Franco, Nat'l Cmty. Reinvestment Coal., HOLC "REDLINING" MAPS: THE PERSISTENT STRUCTURE OF SEGREGATION AND ECONOMIC INEQUALITY 4 (2018), https://ncrc.org/wp-content/uploads/dlm_uploads/2018/02/NCRC-Research-HOLC-10.pdf.
[11] Letter from LDF & Student Borrower Protection Ctr. to Dave Girouard, CEO of Upstart Network, Inc. (Jul. 30, 2020), https://www.naacpldf.org/wp-content/uploads/2020-07-30-FINAL-Demand-Letter.pdf (Upstart Demand Letter).
[12] *Id.*

- *Incomplete or Unrepresentative Data:* An ADS can also lead to algorithmic bias if it is trained on incomplete or unrepresentative data.[13] For example, research by Joy Boulamwini, a researcher at the MIT Media Lab and the founder of the Algorithmic Justice League, found that facial recognition algorithms, which were trained on data sets that included primarily white men, were less accurate at identifying faces with darker complexions, and were particularly bad at identifying darker-skinned women.[14] Similarly, a 2019 study by the National Institutes of Science and Technology found that facial recognition systems generally work best on middle-aged white men's faces and were less able to accurately identify Black, Asian, and Native American faces.[15] The study found that these systems generated a large number of false positives, meaning that these systems were significantly more likely to misidentify Black, Asian, and Native American faces.[16]

- *Systemic Discrimination:* ADSs can replicate systemic discrimination that is reflected in the underlying data used to develop the algorithm. The data used to develop and train ADSs is often drawn from existing data sets—for example, current employees or existing borrowers.[17] As such, according to FTC Commissioner Rebecca Slaughter, these systems may reflect "problematic human biases" and "historical and enduring patterns of prejudice or inequality" that exist in that data.[18] For example, automated valuation models for housing may reflect biases that exist in the housing market due to historical and current patterns of discrimination, such as the undervaluation of homes in formerly redlined areas[19] and ongoing appraisal bias.[20]

---

[13] Nicol Turner Lee, *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms,* BROOKINGS INST. (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/; Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 9, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruitingtool-that-showed-bias-against-women-idUSKCN1MK08G.

[14] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* PROCEEDINGS OF MACHINE LEARNING RESEARCH, vol. 81, 2018 at 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[15] Patrick Grother, Nat'l Inst. of Sci. & Tech, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[16] *Id.*

[17] FTC Commissioner Rebecca Kelly Slaughter, Remarks at UCLA School of Law: Algorithms and Economic Justice (Jan. 24, 2020), https://www.ftc.gov/system/files/documents/public_statements/1564883/remarks_of_commissioner_rebecca_kelly_slaughter_on_algorithmic_and_economic_justice_01-24-2020.pdf

[18] *Id.*

[19] Letter from the Nat'l Fair Hous. Alliance to Consumer Financial Protection Board Director Rohit Chopra, CFPB Outline for the Small Business Advisory Review Panel for the Automated Valuation Model Rulemaking, at 5 (May 13, 2022), https://nationalfairhousing.org/wp-content/uploads/2022/05/NFHA-et-al-Comment-Letter_CFPB-re-AVMs_05-13-2022_FINAL.pdf.

[20] *Id.*; *see also, e.g.,* Debra Kamin, *Widespread Racial Bias Found in Home Appraisals*, N.Y. TIMES, Nov. 2, 2022, https://www.nytimes.com/2022/11/02/realestate/racial-bias-home-appraisals.html.

This type of bias can occur even if the data set used to train the AI does not include race or other protected characteristics but does include another variable or variables that are correlated with those characteristics.[21] Algorithmic bias can also result from the interaction of several variables that operate together to create a disparate impact.[22]

While machine learning models are designed to learn over time, the algorithm may never interact with counterfactual data that causes it to revise its predictions.[23] Take, for example, an algorithm that predicts which users are most likely to click a link in an advertisement on a social media site. The algorithm sends advertisements for home sales in a wealthier, white neighborhood to white users but not to Black users. Because Black users would never see the advertisment, the ADS never has the opportunity to learn the inaccuracy of its prediction that Black users would not click the link.

Systemic discrimination by an ADS may be compounded by structural, implicit, and explicit biases influencing decision-makers that use ADSs. For example, crime statistics are not objective measures, but are highly influenced by what behaviors and communities police target.[24] A physical fight between students of color at an urban school where police are present may lead to an arrest for assault; a similar fight at a wealthier, whiter school may go unreported.[25] Similarly, because communities of color have a higher police presence, there are more arrests for offenses like drug possession and traffic offenses in those neighborhoods because more police are there to observe them[26]--even though rates of drug use and sales are similar across racial lines.[27] An ADS built using this data risks replicating and amplifying this discrimination.

These different sources of bias can both prejudice groups of people who share particular characteristics compared to other groups and groups who perform worse at evaluating members of one group than another, a characteristic known as differential validity.[28] For example, in the employment context, an algorithm that lacks differential validity may promote an equal number of candidates across racial groups, but fail to accurately identify the top-performing Black candidates while accurately identifying the top-performing white candidates.[29] As a result, more white

[21] *See* Upstart Demand Letter, *supra* note 11; Hurley & Adebayo, *supra* note 9, at 182.
[22] Hurley & Adebayo, *supra* note 9, at 202.
[23] Lee, *supra* note 13; Pauline Kim, *AI and Inequality, in* Kristin Johnson & Carla Reyes, eds., THE CAMBRIDGE HANDBOOK ON ARTIFICIAL INTELLIGENCE & THE LAW (2022).
[24] *Sandhya Dirks, Rising crime statistics are not all that they seem,* NPR (Nov. 3, 2022), (stating that crime data "tells you how police behave as an organization"), https://www.npr.org/2022/11/03/1133790735/rising-crime-statistics-are-not-all-that-they-seem.
[25] *Id.*
[26] *Id.*
[27] DIANE WHITMORE SCHANZENBACH, ET AL., THE HAMILTON PROJECT, INCARCERATION AND PRISONER REENTRY (2016), https://www.hamiltonproject.org/assets/files/12_facts_about_incarceration_prisoner_reentry.pdf.
[28] Testimony of Manish Raghavan before New York City Council Committee on Technology regarding Int. 1894, Nov. 9, 2020, https://mraghavan.github.io/files/int_1894_testimony.pdf.
[29] *Id.*

candidates would get hired because the ADS is better able to identify white candidates with the right combination of skills—even if the employer is equally open to hiring a Black candidate and the Black candidates have the requisite skills for the position.

II. Algorithmic Discrimination, Based on Race and Other Protected Categories, is Prevalent Across Sectors.

ADSs play an increasing role in how Americans learn about and access opportunities and how the government makes decisions. In 2019, approximately 45 percent of 2,000 large mortgage lenders relied on online or app-based lending interfaces to originate mortgages.[30] An estimated ninety percent of landlords use automatically-generated reports for tenant screening.[31] Employers increasingly rely on data analytic tools to make personnel decisions,[32] and job posting and recruiting tools leverage large amounts of personal data to identify and recruit candidates, rather than broadly disseminating information about opportunities.[33] Law enforcement uses algorithms to decide where to deploy their officers and to identify potential suspects.[34] These new technologies are often deployed with little transparency regarding when they are used, what data sources they rely on, how they make decisions, whether they have been independently validated or tested for bias, or why people may be adversely affected.

Unfortunately, ADSs frequently replicate and amplify existing discrimination and bias, denying people of color and other protected classes equal access to housing, credit, employment, and other opportunities,[35] subjecting them to increased law enforcement contact, and potentially endangering their liberty. As discussed below, researchers and litigators have found algorithmic bias across a number of sectors, including lending, housing, employment, health care, and law enforcement. The examples below are illustrative of the problems that have been identified. However, because there is currently no requirement that the companies that design and develop ADSs, or the companies that use them to make decisions, be transparent about the algorithms they use—nor is there a requirement that they test for bias or make the information regarding ADS bias public once it has been discovered—these examples likely underrepresent the pervasiveness of the problem.

[30] Karl Schmeckpeper, et al., *Algorithm Transparency through the Fair Credit Reporting Act (FCRA)*, J. OF SCI. POL'Y & GOVERNANCE, vol. 18, Sept. 2021, https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/schmeckpeper_etal_jspg_18-4.pdf.
[31] *Id.*
[32] *See* Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 860 (2017).
[33] Karl Schmeckpeper, et al., *supra* note 30.
[34] *See, e.g.,* TIM LAU, BRENNAN CTR. FOR JUST, PREDICTIVE POLICING EXPLAINED (2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
[35] Meredith Broussard, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 115 (2018).

A. *Lending*

Algorithmic bias can deprive people of fair access to credit, leading them to pay more for a mortgage, credit card, or other loans or denying them access entirely. Financial technology, known as "fintech," seeks to apply AI and other new technologies to the production or provision of financial products and services.[36] While fintech has the potential to increase credit access for people of color, research has found that ADSs can still result in racial bias or discrimination.

ADSs have the potential to lead to more fair decision-making[37] by eliminating human bias and expanding access to credit through the use of "alternative data."[38] "Alternative data" can include factors such as social media use, educational attainment, work history,[39] and even factors like "how quickly a loan applicant scrolls through an online terms-and conditions disclosure."[40] For example, both Freddie Mac[41] and Fannie Mae[42] now give borrowers and lenders the option of submitting rental payment history for consideration as part of the entities' automated mortgage underwriting system. The hope is that this additional information will help expand access to credit and homeownership among people of color, whom Fannie Mae found "are disproportionately represented among the 20% of the U.S. population having little to no established credit history."[43] In addition to determining whether to offer a loan and on what terms, companies have also begun using ADSs that track consumer behavior to dynamically adjust their access to credit.[44] However, exactly what data fintech algorithms use and how they use it is often considered proprietary and protected from disclosure.[45] As such, it is difficult to validate whether lenders that rely on

[36] Fair Hou. Finance Agency, FINTECH IN HOUSING FINANCE: REQUEST FOR INFORMATION (2022), https://www.fhfa.gov/PolicyProgramsResearch/Programs/Documents/Fintech-in-Housing-Finance-Request-for-Information.pdf.
[37] Katie Jensen, *Fintech Mortgage Proven To Reduce Racial Bias In Lending*, NAT'L MORTGAGE PROFESSIONAL (Nov. 19, 2021), https://nationalmortgageprofessional.com/news/fintech-mortgage-proven-reduce-racial-bias-lending.
[38] Christopher K. Odinet, *The New Data of Student Debt*, 92 S. CAL. L. REV. 1617, 1673 (2019).
[39] Lorena Rodriguez, *All Data Is Not Credit Data: Closing The Gap Between The Fair Housing Act And Algorithmic Decisionmaking In The Lending Industry*, 120 COLUMBIA L. REV. 1843, 1858-59 (2020), https://deliverypdf.ssrn.com/delivery.php?ID=173022101119067100064082026115113064057072038035075028088072119101005121006005030111124122127028018042026073113105016020012097060013004075058100115094083076122008080085079001123092082003100120005030030069087001088079113082072023112016083070024123069073&EXT=pdf&INDEX=TRUE.
[40] Hurley & Adebayo, *supra* note 9, at 166 tbl. 1.
[41] *Freddie Mac Takes Further Action to Help Renters Achieve Homeownership*, FREDDIE MAC (June 29, 2022 10:00 ET), https://www.globenewswire.com/news-release/2022/06/29/2471417/0/en/Freddie-Mac-Takes-Further-Action-to-Help-Renters-Achieve-Homeownership.html.
[42] *FHFA Announces Inclusion of Rental Payment History in Fannie Mae's Underwriting Process*, FED. HOUSING FINANCE AGENCY (Aug. 11, 2021), https://www.fhfa.gov/mobile/Pages/public-affairs-detail.aspx?PageName=FHFA-Announces-Inclusion-of-Rental-Payment-History-in-Fannie-Maes-Underwriting-Process.aspx.
[43] Hugh R. Frater, *Helping Renters Unlock the Door to Homeownership* (Aug. 11, 2021), https://www.fanniemae.com/research-and-insights/perspectives/helping-renters-unlock-door-homeownership.
[44] Hurley & Adebayo, *supra* note 9, at 150-151.
[45] Rodriguez, *supra* note 39, at 1858.

alternative data really do expand access to credit or accurately assess credit-worthiness.[46] For example, American Express reportedly cut a Black businessman's credit limit by more than 65 percent because "[o]ther customers who ha[d] used their card at establishments where [he] recently shopped have a poor repayment history with American Express."[47] As lenders begin to adopt the use of alternative data, they must ensure that the data used actually expands access to credit, rather than discriminating against particular groups.

An example of how fintech algorithms can discriminate against people of color was revealed in 2020, when the Student Borrower Protection Center (SBPC) tested a lending algorithm developed by a company called Upstart that incorporated educational data—including where the borrower attended college and the average SAT and ACT scores for different colleges and universities.[48] Upstart's algorithm divided schools into tiers based on standardized test scores.[49] The higher the incoming class's average standardized test scores, the higher the school's tier, and the more favorable the terms offered to students who attended that school.[50] Because students of color perform worse on these standardized tests due to embedded biases in those tests, schools with higher percentages of students of color were assigned to lower tranches.[51] For example, "only nine percent of Black students, eight percent of Indigenous American students, and twelve percent of Latin[x] students attend America's most elite public universities."[52] Ninety-five percent of Historically Black Colleges and Universities (HBCU) were in the bottom rankings; just two were in the top tier.[53] In practice, this translated into substantially different loan terms for borrowers of color: A hypothetical graduate of the well-known HBCU Howard University, who applied for a loan through Upstart's lending platform, was charged nearly $3,499 more over the life of a five-year loan than a similarly-situated graduate of New York University, a predominantly white institution.[54]

LDF and SBPC sent a demand letter to Upstart outlining how its algorithm likely violated the Equal Credit Opportunity Act and the Fair Housing Act.[55] In response, Upstart agreed to a fair lending monitorship.[56] As part of this monitorship, Upstart has undergone independent audits of its lending algorithm. In its latest report, the monitor, Relman Colfax, uncovered ongoing

[46] Hurley & Adebayo, *supra* note 9.
[47] Ron Lieber, *American Express Kept a (Very) Watchful Eye on Charges*, N.Y. TIMES (Jan. 30, 2009), https://www.nytimes.com/2009/01/31/your-money/credit-and-debit-cards/31money.html?pagewanted=all.
[48] Student Borrower Protection Ctr., EDUCATIONAL REDLINING 16 (2019), https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf (EDUCATIONAL REDLINING); Upstart Demand Letter, *supra* note 11.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *See* EDUCATIONAL REDLINING, *supra* note 48, at 9.
[53] Upstart Demand Letter, *supra* note 11.
[54] *See* EDUCATIONAL REDLINING, *supra* note 48, at 18.
[55] Upstart Demand Letter, *supra* note 11.
[56] Press Release, LDF & Student Borrower Protection Ctr., NAACP Legal Defense and Educational Fund and Student Borrower Protection Center Announce Fair Lending Testing Agreement with Upstart Network (Dec. 1, 2020), https://protectborrowers.org/naacpldf-sbpc-upstart-agreement/.

algorithmic bias and identified less discriminatory alternative lending models.[57] However, because Upstart had updated its model before the report came out, the monitor ultimately recommended that the company adopt the fair lending methodologies it identified rather than a particular model.[58] These methodologies include proactively "identifying whether statistically and practically significant disparities exist for protected classes, ensuring the existence of a legitimate business need, and searching for less discriminatory alternative models," "report[ing] to the Monitor the results of its application of these methodologies and constraints as it applies them," and ensuring that its process is "repeatable and verifiable by the Monitor."[59] LDF's work to ensure compliance with the monitorship is ongoing.

Researchers have found similar issues of algorithmic bias in other lending algorithms. A recent study by researchers at the University of California - Berkeley examined the practices of six fintech lenders, which they defined as lenders with a strong online presence where nearly all of their mortgage application processes took place online and applications were evaluated using an algorithm with no human involvement from the lenders.[60] The study found that, while the algorithmic lending platforms it tested discriminated 40 percent less than face-to-face lenders, "Latinx and African-American [borrowers] pay 5.3 basis points more in interest for purchase mortgages and 2.0 basis points for refinance mortgages originated on FinTech platforms."[61]

B. *Tenant Screening*

Algorithmic bias can also deny people the ability to rent housing. According to a 2017 survey from TransUnion, which offers a popular tenant screening product, nine in 10 landlords use tenant screening reports to evaluate prospective tenants.[62] These screening reports frequently include an algorithmically-generated score or a recommendation to accept or reject an applicant, inviting landlords to rely on this recommendation rather than making an individualized determination based on the details of a particular application.[63] Yet many tenant screening algorithms rely on variables that are highly correlated with race due to past and ongoing discriminatory policies and

[57] Relman Colfax PLLC, FAIR LENDING MONITORSHIP OF UPSTART NETWORK'S LENDING MODEL: THIRD REPORT OF THE INDEPENDENT MONITOR (2022), https://www.relmanlaw.com/media/news/1332_PUBLIC%20Upstart%20Monitorship%203rd%20Report%20FINAL.pdf
[58] *Id.*
[59] *Id.*
[60] Robert Bartlett, et al., *Consumer-Lending Discrimination in the FinTech Era*, UC BERKELEY PUB. LAW RES. PAPER, at 5 (Nov. 2019), https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf.
[61] *Id.* at 6.
[62] Press Release, TransUnion, Low Turnover and Higher Rental Prices in 2017 Driving Profitable and Attractive Market for Landlords (April 19, 2017 06:00 ET), https://www.globenewswire.com/news-release/2017/04/19/963170/0/en/Low-Turnover-and-Higher-Rental-Prices-in-2017-Driving-Profitable-and-Attractive-Market-for-Landlords.html.
[63] Kaveh Waddell, *How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times*, CONSUMER REPORTS (Mar. 11, 2021, https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/.

practices, such as eviction history or past arrests or convictions, leading to disparate impacts on renters of color.[64] Moreover, in some cases, the information reported by these tenant screening algorithms is not accurate, and the inaccurate information is disproportionately ascribed to people of color. According to an investigation by *The Markup* and the *New York Times*, these reports can include criminal or eviction records from different people with similar names—a problem that occurs more frequently with Black or Latinx applicants.[65]

Recent litigation by the Connecticut Fair Housing Center against CoreLogic Rental Property Solutions demonstrates the risk of algorithmic bias in tenant screenings.[66] When Carmen Arroyo applied to rent an apartment for herself and her son, she agreed to a tenant screening check by the management company.[67] The management company used CoreLogic's program CrimSAFE, which CoreLogic marketed as an "automated tool [that] processes and interprets criminal records and notifies leasing staff when criminal records are found that do not meet the criteria you establish for your community."[68] CoreLogic provided housing providers with a form that listed general categories of crimes for which the algorithm should screen.[69] The program would then return a one-page report indicating whether disqualifying records were found.[70] The Department of Housing and Urban Development had issued guidance stating that using criminal history, particularly prior arrests that did not result in convictions, to screen individuals from housing may be illegal under the Fair Housing Act due to racial disparities in the criminal justice system, and recommending that housing providers conduct an individualized assessment of each tenant.[71] However, the CrimSAFE report provided no additional information to the housing providers, such as the underlying records, the nature of the alleged crime, the date of the offense, or the outcome of the case, if any.[72] After CoreLogic performed the tenant screening for Ms. Arroyo's son using CrimSAFE, it informed the management company that her son was disqualified from tenancy based on unspecified criminal records.[73] Relying on the CrimSAFE report, the management company told Ms. Arroyo that her son was not qualified for tenancy.[74] Ms. Arroyo disputed his exclusion, pointing out that Mr. Arroyo's arrest had occurred two years prior and the charges had subsequently been withdrawn.[75] The Connecticut Fair Housing Center sued CoreLogic on behalf of Ms. Arroyo, arguing that CrimSAFE violated the Fair Housing Act, among other laws.[76] In

[64] *Id.*
[65] Lauren Kirchner & Matthew Goldstein, *How Automated Background Checks Freeze Out Renters*, N.Y. TIMES (May 28, 2020), https://www.nytimes.com/2020/05/28/business/renters-background-checks.html.
[66] *See*, *e.g. Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Solutions*, 369 F. Supp. 3d 362 (D. Conn. 2019)
[67] *Id.* at 367.
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] U.S. Dep't of Hous. & Urban Dev., *Office of General Counsel Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions* (Apr. 4, 2016), https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.
[72] *Conn. Fair Hous. Ctr.,* 369 F. Supp. 3d at 367.
[73] *Id.*
[74] *Id.*
[75] *Id.* at 267-68.
[76] *Id.*

March 2019, the U.S. District Court for the District of Connecticut found that Ms. Arroyo had stated a viable claim under the Fair Housing Act,[77] and, in 2020, that the case could proceed to trial.[78] As of November 4, 2022, the case was still in active litigation.[79]

C. *Housing Advertisements*

Algorithmic bias can also deny people access to fair housing by preventing them from learning about available housing opportunities. For example, algorithms used to distribute housing advertisements online have been found to allow advertisers to exclude people of color from their target audience. In 2016, ProPublica was able to purchase dozens of home-rental ads on Facebook that specifically excluded "African Americans, mothers of high school kids, people interested in wheelchair ramps, Jews, expats from Argentina and Spanish speakers."[80] After conducting its own investigation, the Department of Housing and Urban Development filed a complaint against Facebook (now Meta), which argued that Facebook enabled advertisers to exclude users from receiving housing-related ads based on the recipient's race, color, religion, sex, familial status, national origin, and disability.[81] Civil rights groups, fair housing organizations, and other advocates also filed lawsuits, which were settled after Facebook agreed to establish a separate portal for housing, employment, and credit advertising, and to eliminate options that allowed advertisers to discriminate based on protected characteristics.[82] However, the Department of Justice found that "after Facebook had claimed that it changed its system to address discriminatory ad targeting, would-be advertisers still were able to select targeting options Facebook claimed it had removed."[83] The Department of Justice filed and settled a suit against Meta in June 2022, claiming that it violated the Fair Housing Act.[84] As part of this settlement, Facebook must develop a new system to address disparities between advertisers' audiences and the group of Facebook users who receive the ads, and must submit reports to an independent, third-party reviewer who will audit Facebook's compliance on an ongoing basis.[85]

---

[77] *Id.*
[78] *Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Solutions*, 478 F. Supp.3d 259 (D. Conn. 2020).
[79] U.S. District Court for the District of Connecticut, Public Courtroom Calendar, https://www.ctd.uscourts.gov/courtcalendar/g6pubcal.html?q=1498657238 (last visited Nov. 4, 2022).
[80] Julia Angwin & Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race,* PROPUBLICA (Oct. 28, 2016 1:00 PM ET), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race; *see also* Compl., *United States v. Meta Platforms, Inc.,* No. 22-cv-05187 (S.D.N.Y. Jun. 21, 2022), https://www.justice.gov/opa/press-release/file/1514026/download.
[81] *U.S. Dep't of Hous. & Urban Dev. v. Facebook,* FHEO No. 01-18-0323-8 (HUD Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.
[82] ACLU, Summary of Settlements Between Civil Rights Advocates and Facebook (Mar. 19, 2019), https://www.aclu.org/other/summary-settlements-between-civil-rights-advocates-and-facebook (last visited Nov. 4, 2022).
[83] Compl. ¶ 59, *United States v. Meta Platforms, Inc.,* No. 22-cv-05187 (S.D.N.Y. Jun. 21, 2022), https://www.justice.gov/opa/press-release/file/1514026/download.
[84] *Id.*
[85] Settlement Agreement, *United States v. Meta Platforms, Inc.,* No. 22-cv-05187 (S.D.N.Y. Jun. 21, 2022), https://www.justice.gov/opa/press-release/file/1514031/download.

Other studies have also found that Facebook's ad delivery system disparately harms people of color. For example, a 2019 study by a team at Northeastern University found that "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."[86] Specifically, "broadly and inclusively" targeted Facebook ads about homes for sale were shown to more white users, while ads for rentals were shown to more people of color.[87] The researchers concluded that this skew was not the result of how users responded to the ad, but was likely automated by Facebook based on the content of the ad itself.[88]

D. *Employment*

The use of algorithms can result in discrimination at every stage of the employment relationship. Many employers rely on ADSs at different stages throughout the hiring process, from steering job advertisements toward certain candidates and flagging candidates for recruitment though sites like LinkedIn and Indeed.com, to identifying strong applicants based on analyses of their resumes, and to assessing candidate competencies.[89] In a 2015 survey, 84 percent of employers reported using social media to recruit,[90] and the proportion has likely gone up since then. Researchers at Harvard Business School found that 99 percent of Fortune 500 companies use resume screening tools.[91] Unfortunately, as employment law expert Prof. Pauline Kim has noted, predictive algorithms are likely to reflect existing patterns of occupational segregation.[92] While these patterns are the result of historical and ongoing discrimination and harassment, "the reasons they exist are irrelevant to predictive algorithms."[93] As such, an algorithm that is developed using a data set where people of color are underrepresented among doctors, lawyers, and other professions, or where women are more often nurses and men are more often doctors, will take these observed patterns as a given, resulting in unfair disadvantages for people of color, women, and other protected classes.[94]

---

[86] Muhammad Ali, et al., *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, PROCEEDINGS OF THE ACM ON HUMAN-COMPUTER INTERACTION, vol. 3, Nov. 2019, at 23, https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-muhammad_ali.pdf.
[87] *Id.* at 22-23.
[88] *Id.* at 23.
[89] Alex Engler, *Auditing Employment Algorithms for Discrimination,* BROOKINGS INST. (Mar. 12, 2021), https://www.brookings.edu/research/auditing-employment-algorithms-for-discrimination/.
[90] SHRM, SURVEY FINDINGS: USING SOCIAL MEDIA FOR TALENT ACQUISITION—RECRUITMENT AND SCREENING 3 (Jan. 7, 2016), https://www.shrm.org/hr-today/trends-and-forecasting/researchandsurveys/Documents/SHRM-Social-Media-Recruiting-Screening-2015.pdf; *see also* Aaron Riecke & Mirand Bogen, UPTURN, HELP WANTED: AN EXAMINATION OF HIRING ALGORITHMS, EQUITY, AND BIAS (2018), https://www.upturn.org/work/help-wanted/.
[91] Paul Marks, *Algorithmic Hiring Needs a Human Face*, COMMUNICATIONS OF THE ACM, vol. 65, March 2022, at 17, https://cacm.acm.org/magazines/2022/3/258900-algorithmic-hiring-needs-a-human-face/fulltext#:~:text=What%20is%20known%20is%20that,screening%2C%20the%20Harvard%20team%20report.
[92] Pauline Kim, *Manipulating Opportunity*, 106 VA. L. REV. 867, 897 (2020), https://deliverypdf.ssrn.com/delivery.php?ID=567087069087071071088126071004114125049002010083005045124081093108125018070118089067019011000043062111054092003014070126073090110049062017017095030005078085111088044054117113089111074080082003117094104072087094106113106028123076082064092030013001&EXT=pdf&INDEX=TRUE.
[93] *Id.*
[94] *Id.*

Algorithms used to decide who is shown employment advertisements have repeatedly been shown to discriminate based on race and gender, often reflecting stereotypes about who works certain kinds of jobs. For example, the 2019 Northeastern University study discussed above found widespread disparities in which job advertisements were shown to Facebook users, even when those ads were intended to be shared with broad audiences. Supermarket cashier positions were shown to an audience that was 85 percent women; jobs with taxi companies went to an audience that was approximately 75 percent Black; and jobs in the lumber industry were overwhelmingly shown to men.[95] In a follow-up study, a similar team found that merely removing demographic inputs like gender and age from the targeting criteria failed to prevent the biased distribution of employment ads.[96] An investigation by ProPublica uncovered similar effects.[97] Other studies have found that advertisements promoting science, technology, engineering, and math careers were shown to significantly more men than women.[98]

Similar issues have been found with ADSs used to analyze resumes to identify top candidates to interview. Starting in 2014, Amazon tried to create an AI tool to review the resumes of job applicants to identify candidates to hire as software developers.[99] Unfortunately, because the model was "trained" using resumes submitted to the company over a ten-year period—overwhelmingly from men—it "learned" to systematically downgrade the resumes of women regardless of their qualifications for the job.[100] For example, the ADS penalized resumes that included the word "women's," as in "women's chess club captain," and downgraded graduates of two all-women's colleges.[101] Amazon ultimately discontinued the project.[102]

Several companies also market products to employers that they claim can reliably extrapolate personality traits and predict social outcomes, such as job performance.[103] Some of these tools rely on assessments of observable physical factors like facial or voice recognition,[104] despite the fact

[95] Ali, *supra* note 86, at 20, 30.
[96] Piotr Sapiezynski, et al., *Algorithms That "Don't See Color": Comparing Biases in Lookalike and Special Ad Audiences* (Working Paper No.1912.07579, 2019), https://arxiv.org/pdf/- 1912.07579.pdf.
[97] Ava Kofman & Ariana Tobin, *Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement*, PROPUBLICA (Dec. 13, 2019, 5:00 AM), https://www.propublica.org/article/facebook-ads-can-still-discriminate-againstwomen-and-older-workers-despite-a-civil-rights-settlement.
[98] Anja Lambrecht & Catherine Tucker, *Algorithmic Bias? An Empirical Study of Apparent Gender-Based Discrimination in the Display of STEM Career Ads*, 65 MANAGEMENT SCI. 2966 (2019).
[99] 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-insight-idUSKCN1MK08G.
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] Rebecca Heilweil, *Artificial Intelligence Will Help Determine If You Get Your Next Job*, RECODE (Dec. 12, 2019), https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen.
[104] Riecke & Bogen, *supra* note 90.

that these technologies are less accurate at assessing people with darker skin[105] and the voices of Black people.[106] As such, they may produce inaccurate results for people of color.

E. *Health Care*

Health care providers increasingly rely on algorithms to help diagnose and treat patients, yet these algorithms can lead to Black patients receiving worse care.[107] For example, although Black Americans are four times more likely to have kidney failure, the standard algorithm used around the country to determine transplant list placement explicitly uses race as a factor and puts Black patients lower on the list than white patients, even when all other factors remain identical.[108] Many doctors now believe that the data that led the algorithm's developers to include the race coefficient is actually a reflection of both systemic health disparities and discrimination by providers, and that the continued use of the algorithm leads to worse outcomes for Black patients.[109] A 2019 study similarly found that algorithms intended to identify sicker patients who would benefit from additional care led to Black patients receiving less quality care than their non-Black counterparts.[110] The algorithm used health care costs rather than medical conditions or illnesses to assign risk scores to patients, assuming that the amount of health care spending was correlated with need.[111] However, the study found that Black patients used the health care system overall less than white patients due to bias by health care professionals, lack of communication, or other issues.[112] Black patients who spent the same amount as white patients were therefore often paying for more active interventions, such as emergency visits for complications associated with chronic illnesses like diabetes or hypertension, while the spending of the white patients was largely for routine and preventative care.[113] As a result, although the Black patients had more chronic illnesses, the risk scores calculated by the algorithm for them were on par with those of healthier white people, and the algorithm was less likely to flag eligible Black patients for the high-risk care management they needed.[114]

---

[105] Boulamwini, *supra* note 14.
[106] Allison Koenecke, et al., *Racial disparities in automated speech recognition*, 117 PNAS 7684, https://www.pnas.org/doi/10.1073/pnas.1915768117.
[107] Donna M. Christensen, *Medical Algorithms Are Failing Communities of Color*, HEALTH AFFAIRS (Sept. 9, 2021), https://www.healthaffairs.org/do/10.1377/forefront.20210903.976632/.
[108] Rae Ellen Bitchell & Cara Anthony, *Kidney Experts Say It's Time to Remove Race From Medical Algorithms. Doing So Is Complicated,* HEALTH AFFAIRS (Jun. 8, 2021), https://khn.org/news/article/black-kidney-patients-racial-health-disparities/?utm_campaign=KHN%3A%20Daily%20Health%20Policy%20Report&utm_medium=email&_hsmi=132394588&_hsenc=p2ANqtz--4ODxarsKPHQSQeAfuOeyLJlAbaGTNgUoPyX4KJJqtvaQOUyan-ZRycCujUe8kMR623a6e7lV0KBUtZgGVacR1ynlazQ_Tte4IvXmfHP2n4J1zvI0&utm_content=132394588&utm_source=hs_email.
[109] *Id.*
[110] Ziad Obermeyer et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, SCIENCE, Oct. 2019, at 447, https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-ziad_obermeyer.pdf.
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*

III. Commercially-Developed Technologies, Some of Which Exhibit Algorithmic Bias, Are Also Deployed By Law Enforcement in Ways That Disproportionately Harm People of Color.

Companies also facilitate discrimination by marketing technologies or selling personal data to government agencies such as law enforcement that leads to disparate impacts on people of color. Because of historical and ongoing patterns and practices of discriminatory policing, these technologies are deployed in ways that disproportionately impact people of color and may themselves exhibit algorithmic bias. Companies have overstated the accuracy and effectiveness of these technologies, raising concerns that they are engaging in deceptive practices.

A. *Historic and Current Structural Bias in Policing Practices Influences the Impact of Technologies Sold to Law Enforcement.*

Potential regulations for the commercial sale or transfer of data and technologies by private actors to law enforcement agencies in the United States must take into account the history and current reality of racially-discriminatory policing, the lack of avenues for accountability for officers' abuses of power, and the lack of information available to the public regarding law enforcement officers' exercise of authority and their impact on the public. Law enforcement's criminalization of, and use of brutal force against, Black people in the United States have shaped policing since its very inception.[115] And the harm to Black people intersects with law enforcement's discrimination based on other identities, including sex, gender, gender identity, sexuality, and disability.[116] Nor are these discriminatory police practices relegated to the past, as demonstrated

---

[115] Police forces across the country were created to control the movement of enslaved people, enforced segregation and Jim Crow laws, and used their power to inflict brutal force, and criminalize Black and Brown communities. *See* Olivia B. Waxman, *How the U.S. Got Its Police Force*, TIME (May 18, 2017), https://time.com/4779112/police-history-origins/ (describing connection and similarity between slave patrols and sheriffs during Reconstruction); *see also* Connie Hassett-Walker, *How You Start is How You Finish? The Slave Patrol and Jim Crow Origins of Policing*, AM. BAR ASSOC. (Jan. 12, 2021), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/civil-rights-reimagining-policing/how-you-start-is-how-you-finish/ (history of slave patrols to oppress and control enslaved people in South); Jill Lepore, *The Invention of Police,* NEW YORKER (Jul. 13, 2020), https://www.newyorker.com/magazine/2020/07/20/the-invention-of-the-police (detailing how "[p]rogressive-era policing criminalized blackness"); Elizabeth K. Hinton, AMERICA ON FIRE: THE UNTOLD HISTORY OF POLICE VIOLENCE AND BLACK REBELLION SINCE THE 1960S (2021) (discussing widespread protests in response to police violence and discrimination against Black people).

[116] *See* Trevariana Mason, *Extreme Sentences Disproportionately Impact and Harm Black Women*, NAT'L BLACK WOMEN'S JUST. INST. (Sept. 23, 2021) ("Black women account for roughly 13% of the general population yet account for 29% of incarcerated women."); Nat'l Coal. of Anti-Violence Programs, HATE VIOLENCE: AGAINST TRANSGENDER COMMUNITIES (2013) ("Transgender people of color were 6 times more likely to experience physical violence from the police compared to [w]hite cisgender survivors and victims."); Vilissa Thompson, *Understanding the Policing of Black, Disabled Bodies*, CTR. FOR AM. PROGRESS (Feb. 10, 2021), https://www.americanprogress.org/article/understanding-policing-black-disabled-bodies/#:~:text=In%20the%20United%20States%2C%2050,to%20their%20white%20disabled%20counterparts.

by civil rights lawsuits and federal investigations that have unearthed widespread constitutional violations in communities of color to the present day.[117] In fact, law enforcement activity continues to be concentrated in communities of color, where officers have broad discretion to arrest and use force against the public.[118] At the same time, the public has limited access to information about law enforcement activity and few levers for accountability for any harm caused by officers and law enforcement agencies.[119]

Because law enforcement activity is concentrated in communities of color, agencies have used policing technologies disproportionately on Black and Brown communities to their detriment. People subjected to these technologies are often unaware of the extent to which their private

("In the United States, 50 percent of people killed by law enforcement are disabled, and more than half of [Black people with disabilities] have been arrested by the time they turn 28—double the risk in comparison to their white [counterparts with disabilities].").

[117] *See e.g., Davis v. City of N.Y.*, 10 Civ. 0699 (SAS) (S.D.N.Y. May. 5, 2011) (settlement agreement reached to resolve federal class-action lawsuit brought by individual public housing residents and guests that challenged unlawful police policy and practice of unlawfully stopping and arresting for trespass); *Floyd v. City of N.Y.*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013) (lawsuit that successfully challenged unconstitutional stop-and-frisk policies of racial profiling in New York City); U.S. Dep't of Just., Civil Rights Div., INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT (2016) (concluding that there was reasonable cause to believe that the Baltimore Police Department engaged "in a pattern or practice of conduct that violates the Constitution or federal law") ; U.S. DEP'T OF JUST., CIVIL RIGHTS DIV., INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT (2015) (concluding that Ferguson's law enforcement policies and practices contributed to a pattern of unconstitutional policing); U.S. Dep't of Just., Civil Rights Div., INVESTIGATION OF THE NEW ORLEANS POLICE DEPARTMENT (2011) (concluding New Orleans Police Department officers too frequently use excessive force and conduct illegal stops, searches and arrests with impunity); U.S. Dep't of Just., Civil Rights Div., LAPD NOTICE OF INVESTIGATION LETTER (May 8, 2000) (determining that the LAPD is engaging in a pattern or practice of excessive force, false arrests, and unreasonable searches and seizures in violation of the Fourth and Fourteenth Amendments to the Constitution); *see also* Radley Balko, *There's overwhelming evidence that the criminal justice system is racist. Here's the proof*., WASH. POST (Jun. 10, 2020), https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/#DrugWar (catalog of some evidence of systemic racism in the criminal legal system). In 2019, police killings were the sixth leading cause of death in the United States for young men, but the risk of being killed by the police is more pronounced for Black men, who are 2.5 times more likely than white men to be killed by police. Black women are 1.4 times more likely than white women to be killed by police. *See* Frank Edwards et al., *Risk of being killed by police use of force in the United States by age, race–ethnicity, and sex*, PNAS 16794-95 (2019).

[118] *See, e.g.,* Drew Desilver et al., *10 things we know about race and policing in the U.S.*, PEW RESEARCH CTR. (Jun. 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."); Jeffrey S. Nowacki, *Police discretion, organizational characteristics, and traffic stops: An analysis of racial disparity in Illinois*, 21 INT'L J. OF POLICE SCI. & MGMT. 1, 4-16 (2019), https://journals.sagepub.com/doi/pdf/10.1177/1461355719832617 (noting increased police traffic stops and subsequent charges on Black motorists due to police discretion, prompting the phrase "driving while Black").

[119] *See* Stevie Degroff & Albert Fox Cahn, Surveillance Technology Oversight Project, NEW COPS ON THE BEAT: AN EARLY ASSESSMENT OF COMMUNITY CONTROL OF POLICE SURVEILLANCE LAWS (2021) (noting limited compliance with the few local and state ordinances requiring oversight on police use of technology, as well as the lack of a governing and uniform oversight guidance), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/602430a5ef89df2ce6894ce1/1612984%20485653/New+CCOPS+On+The+Beat.pdf; *see also* Leandra Bernstein, *America has 18,000 police agencies, no national standards; experts say that's a problem*, WJLA (Jun. 9, 2020), https://wjla.com/news/nation-world/america-has-18000-police-agencies-no-national-standards-experts-say-thats-a-problem.

information, including sensitive and identifying data, may be used against them, their families, and people with whom they associate. A person's biometric data, political and religious affiliations, daily movements, social media posts, and other personal information may be bought or acquired by law enforcement agencies and used for law enforcement purposes.[120]

Policing technologies that aid officers' investigations and enforcement activity are often inaccurately promoted as tools that will reduce crime and improve public safety by falsely assuming that officers' investigative and enforcement strategies, which the technologies aid, are effective at improving public safety. On the contrary, many enforcement strategies are counterproductive and fail to address the root causes of crime or violence,[121] while people of color unfairly experience the brunt of police violence and incarceration. Tools that aid law enforcement often increase officers' powers to surveil and perpetuate state violence against people of color without necessarily creating safer communities.[122]

The lack of rules or standards governing commercial technologies sold to law enforcement agencies permits private entities to contribute to the state violence and criminalization that disproportionately harm Black and Brown people. Below are examples of commercial technologies sold to law enforcement agencies, local governments, and school systems. These may initially be sold at deeply discounted prices, which increase steeply after a number of years[123] when agencies and cities often feel dependent on the technologies despite their inefficacy. The law enforcement technologies discussed below are not exhaustive of all such technology that is currently in use to the detriment of communities of color.

---

[120] Law enforcement can and does purchase location data from data brokers. Sara Morrison, *Here's how police can get your data — even if you aren't suspected of a crime*, VOX (Jul. 31, 2021), https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant (describing how law enforcement is increasingly using tactics like reverse search warrants to acquire the data of many people in the hope of finding one or more people suspected of committing a crime).

[121] Juan Del Toro et al., *The criminogenic and psychological effects of police stops on adolescent black and Latino boys*, PNAS 8261 (2019) (finding "[p]olice stops predict decrements in adolescents' psychological well-being and may unintentionally increase their engagement in criminal behavior.").

[122] George Joseph, *What Are License-Plate Readers Good For? Automatic plate-readers catch few terrorists or violent criminals, but do plenty of harm to low-income communities of color*, BLOOMBERG NEWS (Aug. 5, 2016), https://www.bloomberg.com/news/articles/2016-08-05/license-plate-readers-catch-few-terrorists-but-lots-of-poor-people-of-color; Rashida Richardson, et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 NYU L. REV. 192 (2019), https://www.nyulawreview.org/wpcontent/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf; Brian Jefferson, DIGITIZE AND PUNISH: RACIAL CRIMINALIZATION IN THE DIGITAL AGE (2020), https://www.jstor.org/stable/10.5749/j.ctvz0h9s7 ("[d]igital databases, not detention centers . . . are becoming the leading edge of criminal justice in the United States. While more than 2 million people are incarcerated . . . the Bureau of Justice Statistics estimates that 100,596,300 names are stored in criminal history databases. In some cities, 80 percent of the black male population is registered in these databases.").

[123] Bennett Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, ELEC. FRONTIER FOUND. (Aug. 31, 2022) (explaining that Fog Data Science, a data broker company that sells raw location data to federal, state, and local law enforcement agencies, offers initial free trials of their service, followed by a basic service tier of typically 100 queries per month, for $6,000-$9,000 per year, with additional monthly queries for an additional fee).

B. *Gunshot Detection Systems (e.g., ShotSpotter)*

Gunshot detection systems, such as ShotSpotter, are equipped with multiple microphones or acoustic sensors—about 20 to 25 microphones per square mile—that, when placed in a neighborhood, continuously monitor sounds in those areas and, through the use of algorithms, aim to identify the sound of gunfire.[124] When a sound is identified as gunfire, the system creates an alert, and the location of the sound is relayed to law enforcement.[125] When alerted to a shooting, officers may deploy in large numbers, and arrive in residential neighborhoods with their guns drawn and often with an enormous show of force because they believe they are about to meet an armed person.

In many cities, ShotSpotter is overwhelmingly concentrated in communities of color.[126] For example, in Chicago, ShotSpotter is deployed in districts with the highest proportion of Black and Latinx residents.[127] Similarly, in Kansas City, Missouri, "ShotSpotter sensors were installed in a 3.5-square mile swath—about one percent of the city's footprint—that primarily includes neighborhoods where white residents make up as little as 3.5 percent of the population, according to U.S. Census data."[128]

The use of gunshot detection systems increases police enforcement in mostly Black and Brown neighborhoods, subjecting communities of color to the dangers of police stops, frisks, arrests, and even death.[129] As the MacArthur Justice Center noted, "[a]ny resident who happens to be in the vicinity of a ShotSpotter alert will be a target of police suspicion or worse. These volatile deployments can go wrong in an instant."[130] The Chicago Inspector General's analysis of Chicago

[124] Jay Stanley, *Four Problems with the ShotSpotter Gunshot Detection System*, ACLU (Aug. 24, 2021), https://www.aclu.org/news/privacy-technology/four-problems-with-the-shotspotter-gunshot-detection-system.
[125] *Id.*
[126] ShotSpotter's official website states that more than 135 cities have contracted with them. ShotSpotter, https://www.shotspotter.com/shotspotter-cities/ (last visited Nov. 8, 2022); Todd Feathers, *Gunshot-Detecting Tech Is Summoning Armed Police to Black Neighborhoods*, VICE (Jul. 19, 2021), https://www.vice.com/en/article/88nd3z/gunshot-detecting-tech-is-summoning-armed-police-to-black-neighborhoods?fbclid=IwAR3W9CjNa1QVLHk8JrutFG85RKIwHYcBAfuqTRVv5iSziwkh-uyC4sa43qg ("In all four cities, the data shows that the sensors are also placed almost exclusively in majority Black and brown neighborhoods, based on population data from the U.S. Census.") (*Gunshot-Detecting Tech)*; *End Police Surveillance*, MACARTHUR JUST. CTR., https://endpolicesurveillance.com/ (last visited Nov. 4, 2022) ("In Chicago, ShotSpotter is only deployed in the police districts with the highest proportion of Black and Latinx residents. ShotSpotter deployments are concentrated only in those neighborhoods.").
[127] *End Police Surveillance*, *supra* note 126.
[128] *Gunshot-Detecting Tech*, *supra* note 126.
[129] *See End Police Surveillance*, *supra* note 126 (noting that ShotSpotter is deployed overwhelmingly in Black and Latinx neighborhoods in Chicago and that, in over 18 months, it found more than 2,400 stop-and-frisks linked to ShotSpotter, with possible undercounting due to reporting failures).
[130] *Id.;* Stephanie Agnew, *Lawsuit: Chicago Police Department Relies on Faulty "Evidence" from ShotSpotter to Make Arrests*, CHI. APPLESEED (Aug. 24, 2022), https://www.chicagoappleseed.org/2022/08/24/lawsuit-cpd-faulty-evidence-from-shotspotter/.

police data found that merely the "perceived aggregate frequency of ShotSpotter alerts" in some neighborhoods leads officers to engage in more stops and pat downs in those areas.[131]

Moreover, gunshot detection systems do not prevent gun violence and are faulty. First, the systems do not prevent shootings from happening, but merely alert police that sounds similar to gunshots have been heard.[132] Second, while police generally justify the placement of microphones based on prior data of shootings, research has shown the technology has a high false alert rate—meaning, it routinely alerts law enforcement of a shooting, when in fact no shooting has occurred.[133] In Chicago, for example, ShotSpotter falsely alerted officers to a purported shooting *more than 60 times a day*, and at one period had an alarming 87 percent false alert rate.[134] And Chicago is not unique; a number of cities have determined that ShotSpotter creates too many false positives (*i.e.*, reporting gunshots where there were none) and false negatives (missing gunshots that did take place).[135] Additionally, a ShotSpotter expert admitted in a 2016 trial that the company reclassified sounds from a helicopter to a bullet at the request of a police department customer and that such changes occur "all the time" because "we trust our law enforcement customers to be really upfront and honest with us," raising concerns about the objectivity of its data.[136]

---

[131] City of Chi. Off. of Inspector Gen., THE CHICAGO POLICE DEPARTMENT'S USE OF SHOTSPOTTER TECHNOLOGY 19 (2021) ("At least some officers, at least some of the time, are relying on ShotSpotter results in the aggregate to provide an additional rationale to initiate stop or to conduct a pat down once a stop has been initiated.").

[132] Mitchell L. Doucette et al., *Impact of ShotSpotter Technology on Firearm Homicides and Arrests Among Large Metropolitan Counties*, J. OF URB. HEALTH 609 (2021), https://doi.org/10.1007/s11524-021-00515-4 (after examining ShotSpotter in 68 large, metropolitan counties from 1999 to 2016, researchers found that Shotspotter "didn't reduce gun violence or increase community safety" and likely had "no significant impact on firearm-related homicides or arrest outcomes," thus suggesting that "[p]olicy solutions may represent a more cost-effective measure to reduce urban firearm violence").

[133] *ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study*, MACARTHUR JUST. CTR. (May 3, 2021), https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study/ (finding in 21-month study of ShotSpotter deployments from July 1, 2019, to April 14, 2021, "89% turned up no gun-related crime and 86% led to no report of any crime at all" despite "more than 40,000 dead-end ShotSpotter deployments").

[134] Stephanie Agnew, *Lawsuit: Chicago Police Department Relies on Faulty 'Evidence' from ShotSpotter to Make Arrests*, CHI. APPLESEED (Aug. 24, 2022), https://www.chicagoappleseed.org/2022/08/24/lawsuit-cpd-faulty-evidence-from-shotspotter/ ("In Chicago, it was discovered that more than 90% of ShotSpotter alerts lead police to find no evidence to corroborate gunfire when police arrive at the location ShotSpotter sent them: no shooting, no shell casings, no victims, no witnesses, no guns recovered.").

[135] See Donald Maye, *ShotSpotter Accuracy Debate Examined*, IPVM (Jun. 25, 2001), https://ipvm.com/reports/shotspotter-accuracy?code=jsly (noting that the problem "is likely significantly greater than what ShotSpotter insinuates" because the company "uses misleading assumptions and a misleading accuracy calculation" in their advertised accuracy rates); *see also* Dayton (OH) Police Department, ShotSpotter Statement, https://www.daytonohio.gov/DocumentCenter/View/12880/ShotSpotter-Statement-PDF (last visited Nov. 8, 2022); Alejandra Figueroa, *Dayton Police Department won't be renewing ShotSpotter contract for 2023*, WYSO (Oct. 7, 2022), https://news.wosu.org/wyso-stories/2022-10-07/dayton-police-department-wont-be-renewing-shotspotter-contract-for-2023 (Dayton Police Department announcing that it will not be renewing its contract with ShotSpotter, as "it's challenging to develop data showing how effective ShotSpotter is on its own").

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

Despite the unreliability of gunshot detections systems, "ShotSpotter evidence has increasingly been admitted in court cases around the country, now totaling some 200 [cases]."[137] Michael Williams, a 65-year-old man, spent 11 months incarcerated on murder charges based, in part, on purported evidence from ShotSpotter before prosecutors dismissed charges against him.[138] A class action lawsuit has been filed against the City of Chicago for harm caused through the Chicago Police Department's use of ShotSpotter, alleging that the City and police department's use of the faulty and ineffective technology has resulted in systemic violations of residents' constitutional rights.[139]

C. *Surveillance Cameras and Facial Recognition Technology*

The sale to law enforcement of a network of surveillance cameras results in heightened surveillance of predominantly Black and Brown communities.[140] Atlanta, nicknamed "the Black Mecca"[141] due its large Black population, is the most surveilled city in the United States.[142] Similarly, despite the size of New York City's five boroughs, the New York City Police Department's surveillance cameras are concentrated in the neighborhood of East New York, Brooklyn, where more than 90 percent of residents are Black or Hispanic.[143]

---

[137] Garance Burke et al., *How AI-powered tech landed man in jail with scant evidence*, ASSOC. PRESS (Mar. 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220.

[138] *Police Jailed a Man for Murder; Algorithm Was Key Evidence*, ASSOC. PRESS (Mar. 5, 2022), https://www.usnews.com/news/best-states/illinois/articles/2021-08-19/police-jailed-a-man-for-murder-algorithm-was-key-evidence.

[139] *See* Compl., *Lucy Parsons Labs et al., v. City of Chicago et al.*, No. 22-cv-3773 (N.D. Ill. Jul. 21, 2022), https://www.macarthurjustice.org/wp-content/uploads/2022/07/Complaint-file-stamped.pdf ("Every day in Chicago, Chicago Police Department (CPD) officers are deployed around 100 times to chase down alerts of supposed gunfire generated by ShotSpotter. More than 90% of the time they find no indication of any gun-related incident, according to the City's own data. *The result is more than 31,600 unfounded CPD deployments every year because of ShotSpotter—more than 87 on an average day.*").

[140] Patrick Toomey & Ashley Gorski, *The Privacy Lesson of 9/11: Mass Surveillance is Not the Way Forward*, ACLU (Sep. 7, 2021), https://www.aclu.org/news/national-security/the-privacy-lesson-of-9-11-mass-surveillance-is-not-the-way-forward; *What's Wrong With Public Video Surveillance?*, ACLU (Mar. 2002), https://www.aclu.org/other/whats-wrong-public-video-surveillance; *see also* Denise Lavoie, *Court finds Baltimore aerial surveillance unconstitutional*, ASSOC. PRESS (Jun. 24, 2021), https://apnews.com/article/baltimore-courts-503b2eb629abf94c25edf4111baf64bd; Faine Greenwood, *How to regulate police use of drones*, BROOKINGS INST. (Sept. 24, 2020), https://www.brookings.edu/techstream/how-to-regulate-police-use-of-drones/ (describing law enforcement's use of drones to spy on alleged drug deals and homeless encampments, and to arrest three Black Lives Matter protesters).

[141] Teresa Wiltz, *How Atlanta Became a City I Barely Recognize*, POLITICO (Sept. 16, 2022), https://www.politico.com/news/magazine/2022/09/16/atlanta-black-mecca-inequality-00055390 ("Atlanta is, in many ways, the 'Black Mecca[.]'").

[142] Jurgita Lapienytė, *This is the most heavily surveilled city in the US: 50 CCTV cameras per 1,000 citizens*, CYBERNEWS (Sep. 28, 2021), https://cybernews.com/editorial/this-is-the-most-heavily-surveilled-city-in-the-us-50-cctv-cameras-per-1000-citizens/ ("Atlanta is the most surveilled city with a ratio of 48.93 cameras per 1,000 people.").

[143] Sidney Fussell, *The All-Seeing Eyes of New York's 15,000 Surveillance Cameras*, WIRED (Jun. 3, 2021), https://www.wired.com/story/all-seeing-eyes-new-york-15000-surveillance-cameras/#:~:text=NYC's%20most%20surveilled%20neighborhood%20is,nonwhite%2C%20according%20to%20city%20data.

Networked surveillance cameras are frequently purchased by law enforcement agencies and local governments ostensibly to reduce crime, though evidence does not establish that they are effective in this regard.[144] However, research does show that these surveillance cameras increase police surveillance of public activity, have been used to track protestors,[145] and increase the likelihood of police involvement with communities that already bear the burden of disproportionate police violence and incarceration. [146]

Law enforcement agencies have used networked cameras to surveil social justice movements, protestors against police violence, and religious organizations, potentially chilling constitutionally-protected activity.[147] "The FBI has surveilled [B]lack activists and Muslim Americans, Palestinian solidarity and peace activists, Abolish ICE protesters, Occupy Wall Street [protestors], environmentalists . . . ."[148] In 2020, California Highway Patrol surveilled and recorded

---

[144] *See, e.g.,* Jennifer King et al., THE SAN FRANCISCO COMMUNITY SAFETY CAMERA PROGRAM - AN EVALUATION OF THE EFFECTIVENESS OF SAN FRANCISCO'S COMMUNITY SAFETY CAMERAS (2008) (The City of San Francisco found no evidence of their Community Safety Camera program, which installed surveillance cameras at fixed locations to film public streets, sidewalks and common areas of public housing complexes, having an impact on violent crime); Aundreia Cameron et al., *Measuring the Effect of Video Surveillance on Crime in Los Angeles. Prepared for the California Research Bureau*, University of Southern California. School of Policy, Planning, and Development, CRB-08-007, 53 (May 5, 2008), https://popcenter.asu.edu/sites/default/files/210-Cameron.pdf (cautioning policymakers that they should not presume from the use of CCTV cameras "that crime reduction or prevention will occur automatically – or at all" and that cameras are, at best, a tool for law enforcement, "not a panacea.").

[145] Nathan Sheard, *San Francisco Police Illegally Used Surveillance Cameras at the George Floyd Protests. The Courts Must Stop Them*, Electronic Frontier Foundation DeepLinks Blog (Jan. 13, 2022), https://www.eff.org/deeplinks/2022/01/san-francisco-police-illegally-used-surveillance-cameras-george-floyd-protests (stating that the Electronic Frontier Foundation and the ACLU filed suit against the San Francisco Police Department for surveilling thousands of Bay Area residents protesting against police violence).

[146] Ashley Del Villar & Myaisha Hayes, *How Face Recognition Fuels Racist Systems of Policing and Immigration — And Why Congress Must Act Now*, ACLU (Jul. 22, 2021), https://www.aclu.org/news/privacy-technology/how-face-recognition-fuels-racist-systems-of-policing-and-immigration-and-why-congress-must-act-now ("Face recognition technology is . . . used by police departments to wrongfully arrest Black men, by ICE and CBP to target and track immigrant families, and by the FBI to surveil Black Lives Matter demonstrators exercising their First Amendment rights."); *see also* Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SITN (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[147] Andrea Dennis, *Mass Surveillance and Black Legal History*, AM. CONST. SOC'Y (Feb. 18, 2020), https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/; *The U.S. Has More Surveillance Cameras Per Person Than China, New Study Shows*, INVERSE, https://www.inverse.com/article/61552-united-states-china-surveillance-cameras (last visited Oct. 27, 2022) (noting that there is "no question that the proliferation of cameras in our public spaces has the real potential to invade privacy and chill people from exercising their constitutionally-protected rights, like free speech and association").

[148] 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 (explaining how the Federal Bureau of Investigation has "used its ample investigative powers not to suppress violence, but to inhibit the speech and association rights of Black activists"); *see also* Alice Speri, *The FBI Has a Long History of Treating Political Dissent as Terrorism*, INTERCEPT (Oct. 22, 2019), https://theintercept.com/2019/10/22/terrorism-fbi-political-dissent/; Nicole Turner Lee & Caitlin Chin, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*, BROOKINGS INST. (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ (noting surveillance by New York Police Department (NYPD) and Central Intelligence Agency (CIA) of "Muslim neighborhoods, restaurants, mosques, stores, and student groups for over six years after September 11, 2001").

"protesters for racial justice in cities up and down the state" with surveillance cameras placed in low-flying helicopters.[149] One resident described the police presence during the protest as "psychological warfare," noting that "the protests were very peaceful and it was mostly young people, kids in attendance . . . but many people got scared off by the police aggression and helicopters, and it felt like the goal of the low-flying choppers was to terrorize people."[150] Similarly, the San Francisco Police Department tapped into a private network surveillance system to monitor the activity of people protesting the violent police killings of Breonna Taylor and George Floyd.[151] A lawsuit filed on behalf of multiple protestors alleged that the government's surveillance made them fearful of attending future protests and made it harder for them to organize and recruit people to participate in future demonstrations.[152]

Networked surveillance cameras are sometimes coupled with facial recognition software, which has been error-prone for people with darker skin, Asian people, as well as people who are transgender or nonbinary.[153] Together, surveillance cameras and facial recognition technology allow law enforcement agencies to surveil and track entire communities. After capturing images from a surveillance camera, police may run a captured image against any number of databases using a facial recognition algorithm—both public and private—in an attempt to identify the person(s) on the surveillance cameras. This commonly includes Department of Motor Vehicles databases and databases of jail booking photos.[154] Surveillance cameras coupled with facial recognition technology are also employed by federal law enforcement agencies, including the U.S. Immigration and Customs Enforcement (ICE), U.S Customs and Border Protection (CBP),[155] and the Federal Bureau of Investigation (FBI).[156] It is estimated that almost half of American adults—

---

[149] Matt Cagle, *Recordings Show the California Highway Patrol's Aerial Surveillance of Racial Justice Protests*, ACLU (Nov. 16, 2021), https://www.aclusocal.org/en/news/recordings-show-california-highway-patrols-aerial-surveillance-racial-justice-protests.

[150] *Id.*

[151] *SFPD Violated Surveillance Law by Spying on Protests for Black Lives*, ELECTRONIC FRONTIER FOUNDATION (Aug. 15, 2022), https://www.eff.org/press/releases/eff-aclu-brief-sfpd-violated-surveillance-law-spying-protests-black-lives.

[152] Br. of Plaintiffs and Appellants Hope Williams, Nathan Sheard, & Nestor Reyes, *Williams et al. v. City and County of San Francisco*, Cal. App. (Aug. 15, 2022) at 47, https://docs.reclaimthenet.org/williams_v_sf_appeal_brief.pdf ("Plaintiffs are fearful about attending future protests. . . . Plaintiffs will find it more difficult to organize successful protests in the future.").

[153] Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (Jul. 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (Jul. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched28; Joy Buolamwini, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING 1, 1–15 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[154] Drew Harwell, *FBI, ICE Find state driver's license photos are a gold mine for facial-recognition searches*, WASH. POST (Jul. 17, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[155] Johana Bhuiyan, *A US surveillance program tracks nearly 200,000 immigrants. What happens to their data?,* GUARDIAN (Mar. 14, 2022), https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap.

[156] Jay Stanley & Nicola Morrow, *ACLU Seeks Information on Government's Aerial Surveillance of Protesters,* ACLU (Aug. 4, 2020), https://www.aclu.org/news/national-security/aclu-seeks-information-on-governments-aerial-surveillance-of-protesters ("The government is using a deeply invasive, coordinated aerial surveillance campaign to

over 117 million people, as of 2016—have photos within a facial recognition network used by law enforcement.[157] The use of surveillance cameras, facial recognition software, and databases containing driver's license and state identification photos exposes millions of people to a constant "perpetual line up."[158]

In Detroit's Project Green Light Program, surveillance cameras are placed throughout the city of Detroit—a predominantly Black city[159]—at businesses, apartment complexes, schools, and stop lights.[160] The cameras constantly collect data and surveil residents' daily life.[161] And because Detroit police can run its facial recognition against the entire state of Michigan's driver's licenses, state ID, and criminal databases, they are able to conduct a virtual line up of almost *every* Michigan resident.[162] However, the cameras are not distributed equally: "surveillance correlates with majority-Black areas, avoiding [w]hite and Asian enclaves."[163]

The use of one's photo in these perpetual line-ups often occurs without the consent, or even awareness, of the individuals pictured, creating additional privacy implications.[164] At least one facial recognition technology company, Clearview AI, has contracted with law enforcement agencies across the country and mines public platforms and/or photo databases, such as social media platforms and security footage, for the datasets supporting its technology—all without the captured person's knowledge or consent.[165] A person's face could be used to create and train a

---

monitor Black Lives Matter protests, gather information, and surveil people exercising their First Amendment rights.").

[157] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SITN (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[158] Clare Garvie et al., *The Perpetual Line-Up*, GEO. LAW CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/. There is also a high concentration of Black and Brown people in police-created gang databases. For example, the NYPD maintains a database of 42,000 "gang affiliates"—99 percent Black and Latinx—with no requirements to prove suspected gang affiliation. In fact, certain police departments use gang member identification as a productivity measure, incentivizing false reports. Najibi, *supra* note 157.

[159] *QuickFacts: Detroit city, Michigan*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/detroitcitymichigan,MI/PST045221 (last visited Nov. 1, 2022)

[160] Rebecca Smith, PROJECT GREEN LIGHT: SURVEILLANCE AND THE SPACES OF THE CITY (2021), https://storymaps.arcgis.com/stories/14dd97b35cbb4a4298786c75855f8080

[161] Clare Garvie & Laura M. Moy, *America Under Watch*, GEO. LAW CTR. ON PRIV. & TECH. (May 16, 2019), https://www.americaunderwatch.com/.

[162] Paul Egan, *Never arrested? Michigan State Police still likely has your photo in its database*, DET. FREE PRESS (Mar. 11, 2019), https://www.freep.com/story/news/local/michigan/2019/03/11/michigan-statepolice-facial-recognition-database/3102139002/.

[163] Najibi, *supra* note 157.

[164] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It,* N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[165] Police in Miami worked with Clearview AI, which extracts faceprints without their consent. Connie Fossi and Phil Prazon, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC 6 (Aug. 17, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/ (noting that Miami police worked with Clearview to extract faceprints from billions of people faceprints in a Black-led protest against police violence.) Clearview AI's app carries extra risks because law enforcement agencies are uploading sensitive photos to the servers of a company whose ability to protect its data is untested. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It,* N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; *see also Facial Recognition under Scrutiny As Clearview AI's Practices Ruled Illegal in Canada*, IFSEC GLOBAL (Feb. 16, 2021),

facial recognition algorithm without them ever uploading a photo or consenting to its use.[166] When facial recognition technology is shared with law enforcement agencies, police may run hundreds of thousands of searches for an identification, using any photo, against a broad range of available databases, without those in the database ever being informed of law enforcements' access to these photos or use of such searches.[167] If the technology identifies a match, their identifying biometric information is then available for use across multiple law enforcement agencies at the push of a button.[168]

Though nationwide, police surveillance and use of facial recognition software subjects all who are surveilled to life-altering and irreversible harms, the risk is exponentially higher for Black and Brown residents.[169] Black and Brown residents are uniquely at risk for police misidentification,[170]

https://www.ifsecglobal.com/video-surveillance/facialrecognition-under-scrutiny-as-clearview-ais-practices-ruled-illegal-in-canada/ (ruling by Canadian government that Clearview's collection of biometric information from its citizens without their knowledge or consent is illegal).

[166] Joseph Goldstein & Ali Walker, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database.*, N.Y. TIMES (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[167] Katie Canales, *Thousands of US police officers and public servants have reportedly used Clearview's controversial facial recognition tech without approval*, BUSINESS INSIDER (Apr. 6, 2021), https://www.businessinsider.com/clearview-ai-facial-recognition-thousands-police-departments-2021-4; S.T.O.P. Condemns NYPD for 22K Facial Recognition Searches, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (Oct. 23, 2020), https://www.stopspying.org/latest-news/2020/10/23/stop-condemns-nypd-for-22k-facial-recognition-searches.

[168] For example, the Chicago and Detroit Department camera systems allow officers to run facial recognition software against any captured images. Blair Paddock, *Chicago Police Using Controversial Facial Recognition Tool*, WTTW (Jan. 30, 2020), https://news.wttw.com/2020/01/30/chicago-police-using-controversial-facial-recognition-tool (In a statement, the Chicago Police Department said it is: "using a facial matching tool to sort through its mugshot database and public source information in the course of an investigation triggered by an incident or crime."); Bryce Huffman, *What we know so far about Detroit's controversial use of facial recognition*, BRIDGE DET. (Jul. 22, 2021), https://www.bridgedetroit.com/what-we-know-so-far-about-detroits-controversial-use-of-facial-recognition/ ("Detroit police use facial recognition technology to compare pictures of a suspect with a database of images culled from public records, social media and other sources.").

[169] Robert Williams, a Black man who was wrongfully arrested at his home after Detroit police's use of facial recognition software and surveillance systems, commented that "[a]s any other person would be, I was angry that this was happening to me. As any other [B]lack man would be, I had to consider what could happen if I asked too many questions or displayed my anger openly — even though I knew I had done nothing wrong." Robert Williams, *I was wrongfully arrested because of facial recognition. Why are police allowed to use it?*, WASH. POST (Jun. 24, 2020), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/.

[170] Facial recognition technology frequently misidentifies individuals with darker skin, resulting in higher error rates. According to the National Institute of Standards and Technology, even the top performing facial recognition software algorithms misidentify Black people at a rate five to ten times higher than they do white people. *See* Orion Rummler, *How AI police surveillance treats people of color*, AXIOS (Sept. 7, 2019), https://www.axios.com/2019/09/07/surveillance-people-color-race; Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (Jul. 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

wrongful arrest,[171] lengthy detention periods, and even deadly police violence without having committed a crime.[172]

D. *Student Activity Monitoring Software and Social Media Monitoring*

The development and sale of student activity monitoring software to schools have also created disparate risks of law enforcement contact for students, particularly students of color, students who are low-income, LGBTQ students, and students with disabilities. Through school-issued devices and internet networks equipped with student activity monitoring software, schools may track and share with law enforcement a student's location data, audiovisual data, web browsing data, and device usage.[173] This surveillance is not limited to children who are physically within a school building, but "continues everywhere children carry their school-issued computers and whenever they log into school accounts."[174] When children use school-issued devices after school hours, many schools explicitly rely upon third parties—most often law enforcement—to respond to alerts from student activity monitoring software.[175]

---

[171] Robert Williams, *I was wrongfully arrested because of facial recognition. Why are police allowed to use it?*, WASH. POST (June 24, 2020), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/.

[172] Kade Crockford, *How is Face Recognition Surveillance Technology Racist?*, ACLU (Jun. 16, 2020), https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist; see also Ashley Del Villar & Myaisha Hayes, *How Face Recognition Fuels Racist Systems of Policing and Immigration—And Why Congress Must Act Now*, ACLU (July 22, 2021), https://www.aclu.org/news/privacy-technology/how-face-recognition-fuels-racist-systems-of-policing-and-immigration-and-why-congress-must-act-now.

[173] *Surveillance Self-Defense*, ELECTRONIC FRONTIER FOUND. (Mar. 2, 2020), https://ssd.eff.org/en/module/privacy-students ("Location Data: Tracking students' location using their device's GPS coordinates, Wi-Fi connections, and contactless chips in bus passes/ID cards, potentially both on and off school property. Schools have used this data for automated attendance tracking and management, including for class tardiness and school bus riding, and assigning consequences such as detention. Audiovisual Data: Images, video, and audio of students while they are on school grounds. These can be compared to databases of known audiovisual files to identify a person. Web Browsing Data: Monitoring browsing history keeps a record of everything you read online, every site you access, and every term you search for, and then forwards this information to school administrators, and possibly reviewers employed by the surveillance service company. Device Usage: Some invasive software can capture and keep a record of everything you do on a device (phone or laptop), even the things you type or delete. This can include everything you search for on the Internet, what you post on social media, and messages sent through chat applications. If you log into a website or service (like your email or social media accounts), invasive software may also capture your usernames and passwords.").

[174] Todd Feathers, *Schools Spy on Kids to Prevent Shootings, But There's No Evidence It Works*, VICE (Dec. 4, 2019), https://www.vice.com/en/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works (*Schools Spy*).

[175] Elizabeth Laird et al., HIDDEN HARMS: THE MISLEADING PROMISE OF MONITORING STUDENTS ONLINE 20 (2022) ("37 percent of teachers at schools that use student activity monitoring outside of school hours report that a third party focused on public safety, such as law enforcement, receives alerts from the monitoring system after hours. Forty-four percent of teachers report that one or more students have been contacted by law enforcement because of behaviors flagged by the student activity monitoring system, and 22 percent of students say that they or another student at their school has been contacted by a police officer or another adult.").

Rather than being used to keep students safe by identifying threats or providing mental health support,[176] student activity monitoring software is more frequently used as a disciplinary tool.[177] This practice particularly harms Black students, Hispanic students, students from low-income families, and students with disabilities, who are already disciplined at disproportionately higher rates.[178] Involving law enforcement often escalates the consequences of a child's misconduct from traditional school disciplinary methods, like parental involvement and suspension, to carceral consequences, such as criminal charges, arrests, and incarceration.[179] Accordingly, connecting student activity monitoring systems to law enforcement places already marginalized children at risk of further police interaction and subsequent harm. This is particularly alarming as students are using school-issued devices at an "unprecedented rate,"[180] especially after the spread of COVID-19 forced schools to implement virtual and at-home learning.

Black, Brown, and low-income students are more likely to rely heavily on school-issued devices and, thus, are subject to more surveillance and police involvement in their daily lives than peers who use their own personal devices.[181] As Senators Elizabeth Warren and Ed Markey noted in a congressional report, "[w]hile the intent of these products, many of which monitor students' online activity around the clock, may be to protect student safety, they raise significant privacy and equity concerns."[182] Schools send private student data collected from monitoring software to law enforcement officials, who use it to contact students.[183] This practice has resulted in the

[176] Ctr. for Democracy & Tech, Hidden Harms: The Misleading Promise of Student Activity Monitoring Presentation 52-53 (2022), https://cdt.org/wp-content/uploads/2022/08/Hidden-Harms-The-Misleading-Promise-of-Monitoring-Students-Online-Research-Slides.pdf (78 percent of students reported being "[m]ore careful about what they search online because they know it may be monitored" and 66 percent of teachers reported that students are "less likely to access resources or visit websites that might provide help to them" such as "how to access mental health supports"); Laird et al., *supra* note 175 at 4 (2022) ("From monitoring students' public social media posts to tracking what they do in real-time on their devices, technology aimed at keeping students safe is growing in popularity. However, the harms that such technology inflicts are increasingly coming to light.").

[177] Gennie Gebhart, *Spying on Students: School-Issued Devices and Student Privacy*, ELECTRONIC FRONTIER FOUNDATION (Apr. 13, 2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy.

[178] For example, Black students compose approximately one-third of all students arrested, despite only comprising 16 percent of the nation's student population, and are suspended and expelled from school at three times the rate of their white peers. Julianne Hing, *Race, Disability and the School-to-Prison Pipeline*, COLORLINES (May 13, 2014), https://www.colorlines.com/articles/race-disability-and-school-prison-pipeline.

[179] *See* Laird et al., *supra* note 175, at 15.

[180] Gebhart, *supra* note 177 (noting that one-third of all K-12 students in U.S. schools use school-issued devices).

[181] One in five students using school monitoring software reported that they, or another student they know, were contacted by a police officer or other adult due to concerns about them committing a crime based on something flagged through student activity monitoring. *See* Ctr. for Democracy & Tech, HIDDEN HARMS: THE MISLEADING PROMISE OF STUDENT ACTIVITY MONITORING 52 (2022) (CDT); *see also* Lois Beckett, *Under digital surveillance: how American schools spy on millions of kids,* GUARDIAN (Oct. 22, 2019), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle ("If digital surveillance companies scanning students' emails and chats misinterpret their jokes or sarcasm as real threats, that 'could expose students to law enforcement in a way they have not been in the past.").

[182] Elizabeth Warren & Ed Markey, CONSTANT SURVEILLANCE: IMPLICATIONS OF AROUND-THE-CLOCK ONLINE STUDENT ACTIVITY MONITORING 4 (2022).

[183] *Id.* at 3 ("Several of the companies indicated that in certain cases, flagged activities will result in immediate contact of 'law enforcement and/or [the National Center for Missing and Exploited Children],' or 'police dispatch for a wellness check.' Other companies indicated that some districts opt into immediate contact of law

nonconsensual disclosure of students' sexual orientation and gender identity (i.e., "outing"), as well as more LGBTQ students reporting they are being disciplined or contacted by law enforcement for concerns about committing a crime compared to their peers.[184]

Student activity monitoring software also has detrimental effects on students' free expression, with nearly half of students attending schools that use student activity monitoring software reporting that they are not comfortable expressing their true feelings online when they know they are surveilled and their statements tracked.[185] This chilling effect is even greater among students with disabilities and among students who have been disciplined before.[186]

Overall, school monitoring systems mimic the invasive and harmful effects of police network surveillance, except they target a more vulnerable population: school-aged children. There is no independent evidence that student activity monitoring software improves student safety.[187] On the contrary, studies show that more surveillance in schools *decreases* students' perceptions of safety, equity, and support.[188] Research shows that schools with more students of color are already more likely to adopt stricter and more encompassing surveillance, security, and law enforcement methods.[189] The spread of pervasive student activity monitoring software also threatens to further entrench the disturbing school-to-prison pipeline, where students of color are especially vulnerable to discriminatory policing. By purchasing student activity monitoring software, administrators are investing in oppressive technologies rather than more empirically supported services to create positive school climates.[190]

Similar to student activity monitoring, local, state and federal law enforcement agencies across the country engage in social media monitoring.[191] This occurs through either a formal contract

---

enforcement—either when it is 'the only option available' or when they 'prefer that we contact public safety agencies directly in lieu of a district contact.' These products may be exacerbating the school-to-prison pipeline by increasing the involvement of law enforcement with students.").

[184] CDT, *supra* note 181, at 2.

[185] Laird et al., *supra* note 175, at 22.

[186] *Id.* at 52.

[187] *Schools Spy*, *supra* note 174 ("If there is evidence or research that is available, it's provided by the vendor. It's not provided by an independent researcher.").

[188] Mona Wang & Gennie Gebhart, *Schools Are Pushing the Boundaries of Surveillance Technologies*, EFF (Feb. 27, 2020), https://www.eff.org/deeplinks/2020/02/schools-are-pushing-boundaries-surveillance-technologies; Sarah Lindstrom Johnson et al., *Surveillance or Safekeeping? How School Security Officer and Camera Presence Influence Students' Perceptions of Safety, Equity, and Support*, J. OF ADOLESCENT HEALTH 1 (Sept. 2018).

[189] Melinda D. Anderson, *When School Feels Like Prison*, ATLANTIC (Sep. 12, 2016), https://www.theatlantic.com/education/archive/2016/09/when-school-feels-like-prison/499556/ (discussing study that "found that the concentration of students of color was a predictor of whether or not schools decided to rely on more intense [security] measures").

[190] *See, e.g.,* Cara McClellan, NAACP Legal Defense and Educational Fund, Inc., OUR GIRLS, OUR FUTURE: INVESTING IN OPPORTUNITY & REDUCING RELIANCE ON THE CRIMINAL JUSTICE SYSTEM IN BALTIMORE 2 (2018), *available at* https://www.naacpldf.org/wp-content/uploads/Baltimore_Girls_Report_FINAL_6_26_18.pdf.

[191] Indeed, more than 70 percent of law enforcement agencies across the country use social media as a tool in their investigations. Marco Poggio, *LAPD Case Sheds Light On Agencies' Social Media Monitoring*, LAW360 (Jan. 9, 2022, 8:26 PM EST), https://www.law360.com/articles/1450472/lapd-case-sheds-light-on-agencies-social-media-monitoring. A 2016 survey of 539 law enforcement agencies in 48 states and the District of Columbia found that

between law enforcement and companies that offer social media monitoring software[192] or officers' informal review and subjective determination of public social media posts.[193] A social media profile can reveal an astounding amount of personal information: beliefs, professional and personal networks, health conditions, sexuality, and more. With that in mind, this growing—and largely unregulated—monitoring of social media by the government is rife with risks for one's right to freedom of speech, assembly, and religion, particularly for Black, Latinx, and Muslim communities, who are already targeted more often by law enforcement and intelligence efforts.[194]

While social media monitoring programs may be used against any member of the public, they are often targeted towards youth. A whopping 97 percent of teenagers in America use social media daily—with almost half reporting that they use the internet "almost constantly."[195] Black and Latinx teenagers more frequently reported being on the internet than did white teenagers and were more likely than white teenagers to report that they use at least one of the five largest online social media platforms "constantly."[196] Accordingly, the use of social media monitoring software can lead to disproportionate monitoring of youth of color, wrongful allegations of criminal activity, and dangerous misinterpretations of social media activity.[197] Collectively, student activity and

---

nearly three-quarters of the surveyed agencies used social media to conduct intelligence gathering for investigations. KIDEUK KIM ET AL., 2016 LAW ENFORCEMENT USE OF SOCIAL MEDIA SURVEY 7, 9 (Urb. Inst. 2017), https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf; *see also* Harsha Panduranga & Emil Mella Pablo; *Federal Government Social Media Surveillance, Explained*, BRENNAN CTR. FOR JUST. (Feb. 9, 2022), https://www.brennancenter.org/our-work/research-reports/federal-government-social-media-surveillance-explained#:~:text=social%20media%20surveillance%3F-,Yes.,be%20reported%20to%20law%20enforcement ("The three agencies that use social media the most for monitoring, targeting and information collection are the Department of Homeland Security, the Federal Bureau of Investigation, and the State Department. However, many other federal agencies monitor social media, including the Drug Enforcement Administration, the U.S. Postal Service, the Internal Revenue Service, the Social Security Administration, the U.S. Marshals Service, and the Bureau of Alcohol, Tobacco, Firearms and Explosives.").

[192] Michael Kwet, *ShadowDragon: Inside the Social Media Surveillance Software That Can Watch Your Every Move*, INTERCEPT (Sept. 21, 2021, 9:03 PM), https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/ (reporting on Michigan State Police Department's contract with a social media monitoring software company, ShadowDragon). For a list of known social media monitoring companies and the local, state, and federal agencies that contract with them to use the surveillance software, see Poggio, *supra* note 191.

[193] Some officers simply browse through publicly available social media posts by searching for specific terms, phrases, or hashtags that they believe could elicit association with criminal activity. Rachel Levinson-Waldman & Ángel Díaz, *How to reform police monitoring of social media*, BROOKINGS INST. (July 9, 2020), https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/. If certain posts are not made available to the public, law enforcement officers resort to creating false accounts or using an informant to gain access to private content. *Id.*; *see also* Poggio, *supra* note 191 (discussing "evidence that LAPD officers routinely created fake accounts to investigate criminal suspects and obtain information from people").

[194] Panduranga & Pablo, *supra* note 192.

[195] Emily A. Vogels, Risa Gelles-Watnick, & Navid Massarat, Pew Rsch. Ctr., TEENS, SOCIAL MEDIA AND TECHNOLOGY 8 (Aug. 10, 2022).

[196] *Id.* at 9, 14 (reporting that 45 percent of Black teens and 47 percent of Latinx teens say they are on one of the main five online platforms almost constantly, as compared to 26 percent of white teens, where the five main platforms include YouTube, TikTok, Instagram, Snapchat, and Facebook).

[197] For example, Jelani Henry, a teenager who was wrongly charged with murder based in large part on having been deemed a criminal affiliate after "liking" friends' videos on Facebook, spent two years on Rikers Island awaiting

social media monitoring software contribute to the school-to-prison pipeline by punishing and pushing students out of school and into the criminal legal system.[198]

E. *Predictive Policing*

The development and sale of software marketed as predictive policing software to law enforcement also increases the disparate criminalization of Black and Brown people, especially Black and Brown youth. "Predictive policing" tools attempt to determine whether a crime will be committed, either in a certain location or by a certain person.[199] Misleading terms like "predictive policing," "risk assessments," and "artificial intelligence" create the faulty impression that these tools are objective, unbiased, accurate, and intelligent. However, predictive policing tools do not make predictions of future crime; instead, they predict where future policing will occur, because they make their recommendations using data on prior policing and enforcement activities, including but not limited to police arrest, crime, and gun violence data.[200]

This data reflects crime and police activity that has already occurred, based on biased policing practices, and relies upon this data to make future "predictions" about an individual or a location's likelihood for criminal activity.[201] Despite this inherent bias in the technology, predictive policing

---

trial, including nine months in solitary confinement, until his case was dismissed. Ben Popper, *How the NYPD is Using Social Media to Put Harlem Teens Behind Bars*, VERGE (Dec. 10, 2014), https://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison. Moreover, former acting chief of DHS's Office of Intelligence and Analysis, Melissa Smislova, has noted that "[a]ctual intent to carry out violence can be difficult to discern from the angry, hyperbolic—and constitutionally protected—speech and information commonly found on social media." Panduranga & Pablo, supra note 192.

[198] Mona Wang & Gennie Gebhart, *Schools Are Pushing the Boundaries of Surveillance Technologies*, ELEC. FRONTIER FOUND. (Feb. 27, 2020), https://www.eff.org/deeplinks/2020/02/schools-are-pushing-boundaries-surveillance-technologies (discussing social media filtering technologies employed by some school districts that send automated alerts to school administrators and local police); *School-to-Prison Pipeline [Infographic]*, ACLU https://www.aclu.org/issues/juvenile-justice/school-prison-pipeline/school-prison-pipeline-infographic (describing the disproportionate effects of school disciplinary policies on Black students) (last visited Oct. 28, 2022).

[199] Tim Lau, *Predictive Policing Explained*, BRENNAN CTR. FOR JUST. (April 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained ("Predictive policing involves using algorithms to analyze massive amounts of information in order to predict and help prevent potential future crimes. Place-based predictive policing, the most widely practiced method, typically uses preexisting crime data to identify places and times that have a high risk of crime. Person-based predictive policing, on the other hand, attempts to identify individuals or groups who are likely to commit a crime—or to be victim of one—by analyzing for risk factors such as past arrests or victimization patterns.").

[200] Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm is Fundamentally Flawed*, VICE (Feb. 14, 2019 12:57 PM), https://www.vice.com/en/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed (noting that "[b]ecause this data is collected as a by-product of police activity, predictions made on the basis of patterns learned from this data do not pertain to future instances of crime on the whole," which explains why "predictive policing is aptly named: it is predicting future policing, not future crime").

[201] Lau, *supra* note 199 (describing "how some police departments rely on 'dirty data'—or data that is 'derived from or influenced by corrupt, biased, and unlawful practices,' including both discriminatory policing and manipulation of crime statistics—to inform their predictive policing systems"); *see also* Will Douglas Heaven, *Predictive policing algorithms are racist. They need to be dismantled.*, MIT TECH. REV. (Jul. 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (noting that some pretrial algorithms still use predictors that are out of date, like

systems are still used, and often serve as justification for continued discriminatory policing of Black and Brown communities. For example, an analysis of the predictive policing software PredPol found that the company sent more than 5.9 million crime predictions to law enforcement agencies across the country—including law enforcement in California, Florida, Texas, and New Jersey—with the same recurring patterns.[202] PredPol "predicted" little to no crime in neighborhoods with predominantly white and middle to upper income residents, but, by contrast, PredPol "targeted relentlessly" neighborhoods with predominantly Black, Hispanic, and/or low-income families.[203]

Moreover, the targets of increased policing activity are often unaware that they have been subjected to a predictive policing tool and have no access to the data upon which it relies.[204] The Pasco (Florida) County Sheriff's Office, for example, places students on an "At-Risk Youth" or "At-Risk Target" list created with "algorithmic risk assessment without any notice to parents and guardians, thus identifying them as likely to commit future crimes and then subjecting the identified children to persistent and intrusive monitoring."[205]

IV. Algorithmic Discrimination Harms People Who Are Evaluated by Algorithms, Companies that Rely on Algorithms, and Society as a Whole.

As can be seen in the examples above, algorithmic bias can lead to several distinct forms of harm for individuals, particularly people of color and other protected classes. Algorithmic bias and/or discrimination can also harm the companies that rely on algorithmic decision-making, as well as society as a whole.

---

predicting that a defendant without a landline phone is less likely to show up in court); Dorothy E. Roberts, *Book Review: Digitizing the Carceral State*, 132 HARV. L. REV. 1695, 1708 (2019), https://harvardlawreview.org/wp-content/uploads/2019/04/1695-1728_Online.pdf ("Computerized risk assessments are based on data taken from a social context that has already been shaped by hierarchies of race, class, and gender. Predictive algorithms package this unequal social structure into a score that necessarily reflects individuals' privileged or disadvantaged positions. The aphorism 'garbage in, garbage out' captures an important aspect of data collection but doesn't capture the nature of built-in structural bias. Inequality in, inequality out is more apt.").

[202] Aaron Sankin et al., *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them.*, GIZMODO (Dec. 2, 2021), https://gizmodo.com/crime-prediction-software-promised-to-be-free-of-biases-1848138977 (describing how PredPol recommended police spend more time in the very neighborhoods that were already disproportionately Black, Brown, poor, had experienced increased policing previously, and had most problems with biased policing).

[203] *Id.*; *see also* Heaven, *supra* note 201.

[204] For example, between 2018 and 2021, more than one in thirty-three U.S. residents were potentially subject to police patrol decisions directed by a crime-prediction software called PredPol. Sankin et al., *supra* note 202. Additionally, the NYPD revealed that in 2019, it used ten years of manually collected historical crime data to develop its predictive policing tool, Patternizr, and teach it to detect crime patterns. Rachel Levinson-Waldman & Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, BRENNAN CTR. FOR JUST. (Jan. 26, 2018), https://www.brennancenter.org/our-work/analysis-opinion/court-public-deserves-know-how-nypd-uses-predictive-policing-software.

[205] *See* Petition for Writ of Mandamus at ¶ 16, *CAIR-Florida v. Nocco*, No. 157331829 (Fla. Cir. Ct. filed Sept. 13, 2022); Neil Bedi & Kathleen McGrory, *Pasco's sheriff uses grades and abuse histories to label schoolchildren potential criminals. The kids and their parents don't know*, TAMPA BAY TIMES (Nov. 19, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data/.

People of color who are subject to automated decision-making in economic sectors can experience several different kinds of harm. First, they may never learn of a housing, employment, credit, or other opportunity because they are excluded by an advertising or recruitment algorithm. Second, they may apply for a job or a loan, or seek to rent an apartment, only to have their application rejected based on an ADS's flawed recommendation. Finally, they may be offered what they seek—a loan or insurance—at substantially worse terms than other applicants. All of these harms have significant economic impacts, from disproportionately forcing people of color to pay more for the same products and services to denying them opportunities for better employment or housing. Taken together, these impacts could further deepen the patterns of discrimination that have led to the growing Black-white racial wealth gap.[206]

Law enforcement uses of ADSs likewise subject people of color to significant harm, including psychological trauma from law enforcement encounters, loss of liberty, and even injury or death if a law enforcement encounter turns violent.[207] People who are arrested—even if the charges are subsequently dismissed or result in a non-criminal conviction—also face loss of employment, housing, custody of their children, and other collateral consequences.[208]

Algorithmic bias also harms employers, landlords, and others who use ADSs. Businesses relying on ADSs to accurately identify top job candidates may fail to engage qualified Black job candidates due to a poorly-performing algorithm. Similarly, an algorithm that discriminates by failing to share opportunities with particular groups based on race or other protected characteristics may exclude potential customers. And an algorithm that inaccurately deems a borrower of color too risky will lead lenders to deny loans to viable customers.

Finally, while algorithmic bias, like other forms of discrimination, hurts communities of color most, it hurts society as a whole. For example, a 2020 study by Citi estimates that the United States' aggregate economic output would have been $16 trillion higher since 2000 if we had closed racial gaps in wages, access to higher education, small business lending, and mortgage access.[209] Algorithmic bias could entrench or exacerbate these existing trends. Discrimination by law

---

[206] *Cf.* SHAPIRO, ET AL., *supra* note 10, at 2.

[207] *See, e.g.,* Amanda Geller et al., *Aggressive Policing and the Mental Health of Young Urban Men*, 104 AM. J. PUB. HEALTH 2321, 2321 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4232139/pdf/AJPH.2014.302046.pdf; Fablina Sharara et al., *Fatal police violence by race and state in the USA, 1980–2019: a network meta-regression*, 398 LANCET 1239, 1239 (Oct. 2, 2021), https://www.thelancet.com/action/showPdf?pii=S0140-6736%2821%2901609-3.

[208] *See, e.g.*, Am. Bar Assoc., COLLATERAL CONSEQUENCES OF CRIMINAL CONVICTIONS: JUDICIAL BENCH BOOK 11 (2018), https://www.ojp.gov/pdffiles1/nij/grants/251583.pdf.

[209] Dana M. Peterson & Catherine L. Mann, Citi GPS, CLOSING THE RACIAL INEQUALITY GAPS: THE ECONOMIC COST OF BLACK INEQUALITY IN THE U.S. 7 (2020), https://ir.citi.com/%2FPRxPvgNWu319AU1ajGf%2BsKbjJjBJSaTOSdw2DF4xynPwFB8a2jV1FaA3Idy7vY59bOtN2lxVQM%3D.

enforcement also leads communities of color to rightfully question the lawfulness and legitimacy of police.[210]

V. While Companies and Government Actors May Be Liable for Discrimination Due to Their Use of Algorithms Under Existing Anti-Discrimination Laws, Additional Measures are Needed to Help Identify and Redress Algorithmic Bias.

A. *Discrimination in Economic Sectors*

Companies do not escape liability under existing laws and regulations just because the discrimination results from the use of an algorithm. In a 2017 talk, Maureen K. Ohlhausen, who was then-acting chair of the Federal Trade Commission, suggested analyzing how existing legal regimes apply to algorithms by substituting "a guy named Bob" everywhere the word algorithm appears.[211] As she said, "If it isn't OK for a guy named Bob to do it, then it probably isn't OK for an algorithm to do it either."[212] While Chair Ohlhausen was specifically discussing antitrust liability, the same principle applies to cases of discrimination.[213] As seen in the examples in Section III above, government agencies and advocacy organizations have successfully used existing civil rights laws to litigate algorithmic bias and/or discrimination. Federal regulatory agencies, such as the Equal Opportunity Employment Commission[214] and the Consumer Financial Protection Bureau,[215] have also issued guidance discussing how the Americans with Disabilities Act and the Equal Credit Opportunity Act, respectively, apply to ADSs.

Unfortunately, members of protected classes often face significant obstacles to identifying and responding to algorithmic bias. Currently, there is no requirement that companies relying on ADSs disclose that fact to people affected. As such, individuals may know that they received an adverse decision—i.e., they did not get an interview or were denied a loan—but they may not know that the outcome was the result of an ADS or what factors led to the adverse decision. In the case of advertising and recruiting, they may not know that they received an adverse outcome at all, because they have no way of knowing about opportunities from which they were excluded.

---

[210] *Race, Trust and Police Legitimacy*, NAT'L INST. OF JUST. (Jan. 9, 2013), https://nij.ojp.gov/topics/articles/race-trust-and-police-legitimacy (citing research showing that people of color frequently report discrimination by law enforcement and are more likely than white people to distrust law enforcement).

[211] Maureen K. Ohlhausen, Acting Chairwoman, U.S. Federal Trade Commission, Should We Fear The Things That Go Beep In the Night? Some Initial Thoughts on the Intersection of Antitrust Law and Algorithmic Pricing (Mar. 23, 2017), https://www.ftc.gov/system/files/documents/public_statements/1220893/ohlhausen_-_concurrences_5-23-17.pdf.

[212] *Id.*

[213] *Id.*

[214] Equal Employment Opportunity Commission, *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*, No. EEOC-NVTA-2022-2 (May 12, 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

[215] Consumer Financial Protection Board, Consumer Financial Protection Circular 2022-03 (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/.

Even if someone believes that they were a victim of discrimination, the lack of transparency imposes practical barriers on potential plaintiffs. There is no requirement that designers or developers of ADSs publish their algorithms or share information about what data they used to develop and train the algorithm, how it was validated, whether it has been audited for bias, or the outcome of and response to that audit. In fact, these algorithms are usually considered proprietary.[216] Without access to the algorithm or information about the algorithm, it can be difficult for potential plaintiffs to establish that bias caused the adverse outcome.[217] While advocacy organizations and researchers can try to test a model for bias—for example, by creating different borrower profiles, as in the Upstart case[218]—this process can be resource intensive. It also may not be possible to easily identify algorithmic bias through testing if the bias is the result of the interaction of multiple variables,[219] or if the company does not offer a public platform to use for testing, as was true with Upstart. As such, it may be challenging to plead sufficient facts to make a preliminary showing of disparate impact or disparate treatment. Moreover, there are currently no mandates requiring companies to preserve the ADS as it existed at the time of an adverse decision, potentially preventing harmed individuals from being able to test the model to show algorithmic bias in a specific decision.

Finally, in the absence of comprehensive regulations, ADSs can be quickly deployed and act on large numbers of people at once—for example, by shaping what information is received or hidden from millions of Facebook users.[220] As such, algorithmic bias can cause widespread harm before the discrimination is ever detected.

B. *Discrimination by Law Enforcement Technologies*

There are also significant obstacles to challenging law enforcement uses of ADSs and other surveillance technologies. In addition to the lack of transparency and other issues described in the preceding section, in some cases, the constitutional theories that allow accused individuals to challenge the evidence against them in criminal court do not map easily onto these technologies. For example, individuals may not be able to challenge their identification by facial recognition technology because that evidence will often not come in at trial, even if it is an integral part of the chain of events that led to their arrest.[221] Moreover, individuals' ability to effectively question evidence from ADSs is limited because, as noted above, the algorithms used by these systems are considered proprietary.

---

[216] Rodriguez, *supra* note 39, at 1858.
[217] Hurley & Adebayo, *supra* note 9, at 194.
[218] *See* EDUCATIONAL REDLINING, *supra* note 48.
[219] Hurley & Adebayo, *supra* note 9, at 194.
[220] John Gramlich, *10 facts about Americans and Facebook*, PEW RESEARCH CTR., June 1, 2021, https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/.
[221] Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, THE CHAMPION, July 2019, at 14, https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf.

C. *Potential and Limits of the Blueprint for an AI Bill of Rights*

The White House Office of Science and Technology Policy recently took the positive step of issuing a Blueprint for an AI Bill of Rights that adopts, as one of its principles, that people should "not face discrimination by algorithms and systems should be used and designed in an equitable way."[222] The Blueprint acknowledges that discrimination by algorithms may, in certain circumstances, violate existing laws.[223] It recommends that "designers, developers, and deployers of automated systems should take proactive and continuous measures to protect individuals and communities from algorithmic discrimination and to use and design systems in an equitable way," including conducting proactive equity assessments as part of the system design, using representative and accurate data and protecting against proxies for demographic features, and performing pre-deployment and ongoing disparity testing and mitigation.[224] The Blueprint also describes additional measures that should be taken to ensure adequate notice and explanation regarding the use of algorithms, as well as the availability of human alternatives, consideration, and fallback.[225] Unfortunately, the Blueprint is non-binding and does not mandate that companies take these steps.[226] Moreover, the Blueprint includes exemptions that suggest that current and future uses of ADSs by law enforcement and in national security contexts need not be subjected to the same principles or be weighed differently against law enforcement concerns.[227]

VI. Principles to Guide Future Regulations

The FTC has broad jurisdiction to make rules protecting consumers and governing trade, and that includes conducting a rulemaking in this area under Section 5 of the FTC Act.[228] The FTC should exercise this authority to take steps to enhance existing legal protections against algorithmic bias and protect communities from commercial technologies that perpetuate or exacerbate systemic racial and other bias, including technologies sold to and used by the government. The FTC should also consider using its existing authority to regulate private companies' collection and use of personal data to develop technologies for law enforcement, as well as the sale or transfer of personal data to law enforcement.

As the FTC considers future rulemakings to address these issues, it should adopt the following principles. These principles are intended to provide preliminary guidance, not to provide an exhaustive or exclusive list of recommendations.

---

[222] WHITE HOUSE OFFICE 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 (AI Bill of Rights).
[223] *Id.*
[224] *Id.*
[225] *Id.*
[226] *Id.*
[227] *Id.*
[228] 15 U.S.C. § 45.

First, the FTC should reaffirm that existing civil rights laws—including laws that the FTC enforces, such as the Equal Credit Opportunity Act[229]—apply to algorithmic discrimination and bar the deployment of algorithms that have a disparate impact on protected classes in many cases.

Second, as the FTC develops its proposed rules, it should actively reach out to communities of color and other stakeholder groups who are impacted by algorithmic bias and the discriminatory deployment of technology by law enforcement to solicit their feedback on the harms caused by algorithmic bias, and potential solutions to mitigate or remedy those harms.

Third, because algorithmic bias has the potential to cause widespread harm, the FTC should, to the fullest extent possible under its existing authority, issue regulations to ensure that companies take a number of steps to proactively identify and ameliorate that harm. These steps should include, but not be limited to, the following—many of which have been embraced by the White House's Blueprint for an AI Bill of Rights:[230]

- *Using data that fully and accurately represents the community the ADS will assess when building and testing algorithms*. In order to avoid bias caused by incomplete and unrepresentative data sets, designers and developers must ensure that the ADS is built and tested using data that represents the particular groups of people it will be used to assess. This process should include identifying and correcting systemic bias that is encoded into data due to the history of discrimination in this country—for example, patterns of residential segregation and redlining—that can lead to bias and invalid valuations and assessments.

- *Proactively identifying variables that may lead to biased assessments and outcomes*. For example, Upstart chose to include data on SAT and ACT scores in its lending model, despite research demonstrating that these scores are biased against students of color.[231] Developers and designers must be aware of what biases they are introducing into their models when they include certain variables, carefully weigh the predictive value of that variable against the risk of bias, and consider excluding those variables or including additional variables to address disparities. They should also articulate how the variables are relevant to the target measure (for example, why social media use should affect your ability to repay a loan) before training the model on this data.

- *Using independent auditors to evaluate their algorithms throughout their lifecycle (i.e., during the design stage, pre-implementation, and continuously after release) in order to*

[229] 15 U.S.C. § 1691c(c).
[230] AI BILL OF RIGHTS, *supra* note 222.
[231] Richard V. Reeves & Dimitrious Halikias, *Race gaps in SAT scores highlight inequality and hinder upward mobility*, BROOKINGS INST. (Feb. 1, 2017), https://www.brookings.edu/research/race-gaps-in-sat-scores-highlight-inequality-and-hinder-upward-mobility/.

identify and mitigate discriminatory impacts. ADSs should only be deployed when they advance equity. Independent audits should be conducted to assess whether the ADS disparately harms or disadvantages individuals on the basis of race or other characteristics protected by law. In doing so, companies must acknowledge the ways in which biased data, flaws in the ADS, and the surrounding circumstances can affect their evaluation of how well an ADS performs a task. For example, the data used to evaluate whether an ADS can accurately assess lending risk may itself reflect past discrimination by lenders, and may lack the counterfactual data needed to fully evaluate the model's accuracy, reliability, and validity. Companies should be required to identify and adopt less discriminatory alternatives even if they appear to have lower performance by some narrow measures in order to account for the inherent inefficiencies, inequities, and inaccuracies that result from discrimination, including the costs to businesses and society as a whole. In addition, companies should consider refraining from deploying an algorithm or removing it from use, particularly in those cases where liberty or other significant constitutional rights are at stake. Finally, these audits should examine the accuracy of the ADS overall and whether the model lacks differential validity. Companies should publicly report the findings of these audits, as well as any changes they made to their ADS in response to the findings from these audits. These reports should be in plain language and easily accessible to the public.[232]

- *Increasing transparency about the use, risks, and effects of ADSs.* Companies should publicly disclose when they use ADSs and describe, in plain language, what they are using the algorithm to assess, what variables they are using to make that assessment, where their data is from, and how the model is trained. Companies should also provide detailed notice to people when the use of an ADS has led to an adverse outcome, including stating the basis for that adverse outcome, and explain how to correct the information used in the assessment. Finally, companies should preserve copies of all iterations of their ADS, as well as their audits and adverse outcome notices, to facilitate subsequent regulatory action or litigation.

FTC action on algorithmic bias may overlap with other federal agencies' authority, but any challenges from this overlap can be overcome. For example, a person alleging that a company's algorithm provides inaccurate criminal history information in its tenant screenings may have claims under both the Fair Credit Reporting Act[233] and the Fair Housing Act. However, the Consumer Financial Protection Bureau and FTC do not have authority over the Fair Housing Act, while the Department of Housing and Urban Development does not have authority over the Fair Credit Reporting Act. The fact that the Department of Housing and Urban may enforce a claim under the Fair Housing Act does not diminish the FTC's interest in enforcing a claim under Fair

[232] *Id.* at 5, 23.
[233] 15 U.S.C. §§ 1681-1681x; *see, e.g.,* Compl., *Fed. Trade Commission v. RealPage, Inc*., no. 18-cv-02737-N (N.D. Tex. Oct. 16, 2018), *available at* https://www.ftc.gov/system/files/documents/cases/152_3059_realpage_inc_complaint_10-16-18.pdf.

Credit Reporting Act. In order to navigate these challenges, the FTC should consult with the federal agencies that currently enforce these laws and draw on their civil rights expertise when developing its final rule. However, should the FTC move forward with additional guidance or regulations on algorithmic bias, it will have to develop its own deep expertise and resources in civil rights law in order to be able to effectively regulate and enforce the law in this space. The agency will also need to dedicate resources to civil rights investigations and enforcement.

Finally, the FTC should also address the ways in which private companies facilitate discrimination by other actors, including government actors. The FTC should examine whether certain uses of technology are so lacking in validity and accuracy that marketing these technologies for those uses constitutes a deceptive practice. Further, the FTC should limit the collection; sale and transfer; and use of personal data. Among other steps, the FTC should consider:

- Prohibiting companies from requiring people to sign up for surveillance as a condition for service;
- Requiring companies to provide a plain language explanation of what data is collected and how it is used by the company, both initially and with every update;
- Requiring companies to allow people to opt out of policy updates that allow for increased surveillance or new uses of surveillance;
- Prohibiting the sale of data to government actors, or requiring companies to obtain people's affirmative consent (not in a term of service) before selling their information to government actors;
- Prohibiting the sale of biometric data to all entities, or requiring companies to obtain people's affirmative consent (not in a term of service) before selling their information; and
- Requiring companies to delete data sets and notify customers if their data was already used and sold in violation of these principles.

Again, these recommendations are not meant to be exhaustive. These recommendations also may not be sufficient to address the concerns outlined above about discriminatory law enforcement uses of ADSs and other technologies, and do not address the fundamental question about whether certain technologies create such a significant risk of harm that they should not be used at all. We look forward to further discussions as the FTC considers future rulemakings.

VII. Conclusion

Algorithmic bias in ADSs, as well as the discriminatory deployment of these systems and other technologies, is prevalent across a variety of sectors and can cause significant harm to affected communities, the companies that use ADSs, and society as a whole. We urge the FTC to take action to address these harms.

Thank you for the opportunity to comment. If you have any questions, please contact Amalea Smirniotopoulos, Senior Policy Counsel, at asmirniotopoulos@naacpldf.org; Puneet Cheema, Manager, Justice in Public Safety Project; and Katurah Topps, Policy Counsel, at ktopps@naacpldf.org.

Sincerely,

Lisa Cylar Barrett, Director of Policy and Director of the Washington D.C. Office
Jin Hee Lee, Director of Strategic Initiatives
Amalea Smirniotopoulos, Senior Policy Counsel
Puneet Cheema, Manager, Justice in Public Safety Project
NAACP Legal Defense and Educational Fund, Inc. (LDF)
700 14th Street NW, Suite 600
Washington, D.C. 20005

Katurah Topps, Policy Counsel
NAACP Legal Defense and Educational Fund, Inc. (LDF)
40 Rector Street, Suite #5
New York, NY 10006