# Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform

*Anita L. Allen*

**abstract.** African Americans online face three distinguishable but related categories of vulnerability to bias and discrimination that I dub the "Black Opticon": discriminatory oversurveillance, discriminatory exclusion, and discriminatory predation. Escaping the Black Opticon is unlikely without acknowledgement of privacy's unequal distribution and privacy law's outmoded and unduly race-neutral façade. African Americans could benefit from race-conscious efforts to shape a more equitable digital public sphere through improved laws and legal institutions. This Essay critically elaborates the Black Opticon triad and considers whether the Virginia Consumer Data Protection Act (2021), the federal Data Protection Act (2021), and new resources for the Federal Trade Commission proposed in 2021 possibly meet imperatives of a race-conscious African American Online Equity Agenda, specifically designed to help dismantle the Black Opticon. The path forward requires jumping those hurdles, regulating platforms, and indeed all of the digital economy, in the interests of nondiscrimination, antiracism, and antisubordination. Toward escaping the Black Opticon's pernicious gaze, African Americans and their allies will continue the pursuit of viable strategies for justice and equity in the digital economy.

## introduction

In the opening decades of the twenty-first century, popular online platforms rapidly transformed the world.[1] Digital modalities emerged for communication, business, and research, along with shopping, entertainment, politics, and philanthropy.[2] Online platforms such as Facebook, Twitter, Google, Airbnb, Uber, Amazon, Apple, and Microsoft created attractive opportunities and efficiencies.[3] Today, life without those platforms is nearly unimaginable. But

---

1. *Cf.* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 138-42 (2017) (describing how platforms transformed consumerism and communication).

2. *See* Gaurav Laroia & David Brody, *Privacy Rights Are Civil Rights. We Need to Protect Them.*, FREE PRESS (Mar. 14, 2019), https://www.freepress.net/our-response/expert-analysis/insights-opinions/privacy-rights-are-civil-rights-we-need-protect-them [https://perma.cc/5V66-4CW3] ("For many of us, the internet is our public square, marketplace, employment agency, bank, travel agency, library and theater.").

3. For a description of the benefits of online platforms, see, for example, CHARLTON D. MCILWAIN, BLACK SOFTWARE: THE INTERNET AND RACIAL JUSTICE FROM THE AFRONET TO BLACK LIVES MATTER 5-6, 11 (2020), which observes that social-media platforms offered powerful way to counter images

they come at a heavy price. Familiar platforms based in the United States collect, use, analyze, and share massive amounts of data about individuals—motivated by profit and with limited transparency or accountability.[4] The social costs of diminished information privacy include racial discrimination, misinformation, and political manipulation.[5] This Essay focuses on one set of social costs, one set of institutional failures, and one demographic group: diminished information privacy, inadequate data protection, and African Americans.

African Americans could greatly benefit from well-designed, race-conscious efforts to shape a more equitable digital public sphere through improved laws and legal institutions. With African Americans in mind, there are several reasons for advocating for improved laws and legal institutions. Existing civil-rights laws and doctrines are not yet applied on a consistent basis to combat the serious discrimination and inequality compounded by the digital economy.[6] Existing common law, constitutional law, and state and federal regulations protecting privacy—much of which predates the internet—are of limited value.[7] Current federal privacy and data-protection law—patchy, sectoral, and largely designed to implement 1970s-era visions of fair information practices[8]—is inadequate for digital-privacy protection and equitable platform governance. Although the Federal Trade Commission (FTC) exhibits concern about the special vulnerabilities of African Americans and other communities of color,[9] it has lacked the resources to address many of the privacy-related problems created

---

of Black people as "criminal, intellectually deficient, and culturally deviant" and argues that "[m]astering digital tools has produced the most visible, sustained, and vociferous movement toward racial justice we've witnessed in the United States since the 1960s."

4. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 9 (2015) ("[C]orporate actors have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how they use this knowledge.").

5. *See* Cohen, *supra* note 1, at 152, 157.

6. *See* Becky Cho, Eric Null, Brandi Collins-Dexter & Claire Park, *Centering Civil Rights in the Privacy Debate*, NEW AM. 8 (Sept. 17, 2019), https://d1y8sb8igg2f8e.cloudfront.net/documents/Centering_Civil_Rights_in_the_Privacy_Debate_2019-09-17_152828.pdf [https://perma.cc/MVU7-5ZP2] ("Privacy is not just transactional. Privacy is a civil right."); *see also* Laroia & Brody, *supra* note 2 (discussing new proposed legislation to protect digital-privacy rights and civil rights).

7. *See* Cohen, *supra* note 1, at 152, 181-83 (arguing that litigation under existing law is unlikely to provide meaningful relief for platform users).

8. *See* Robert Gellman, Fair Information Practices: A Basic History 1 (2021) (unpublished manuscript), https://ssrn.com/abstract=2415020 [https://perma.cc/43PR-9DB5] (enumerating fair information practices and their history).

9. *See Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color*, FED. TRADE COMM'N 1-3 (Oct. 2021), https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf [https://perma.cc/BCT9-GSJ9] (detailing Federal Trade Commission (FTC) efforts on behalf of people of color).

by internet platforms.[10] And the platforms themselves have failed to self-regulate in a way that meaningfully responds to race- and equity-related privacy problems.[11] The self-governance efforts and policies adopted by these companies have not silenced criticism that platform firms prioritize free speech, interconnectivity, and interoperability at the expense of equitable privacy protections and antiracist measures.[12]

In the United States, discussions of privacy and data-protection law ground the case for reform in values of individual autonomy, limited government, fairness, and trust—values that are, in theory, appealing to all people.[13] Yet, until recently, the material conditions and interests of African Americans, particularly from their own perspectives, have received limited attention in such discussions. As civil rights advocates observe, although "[p]rivacy should mean personal autonomy and agency . . . commercial data practices increasingly impede the autonomy and agency of individuals who belong to marginalized communities."[14] In pursuit of equitable data privacy, American lawmakers should focus on the experiences of marginalized populations no less than privileged populations. For Black Americans, those experiences feature three compounding vulnerabilities: (1) multiple forms of excessive and discriminatory surveillance; (2) targeted exclusion through differential access to online opportunities; and (3) exploitative online financial fraud and deception. Digital-privacy and data-protection law proposals fashioned to promote equitable governance online must be responsive to calls for improved online governance made by and on behalf of African Americans relating to these forms of pervasive and persistent disadvantage.

Although a great deal of state and federal privacy and data-protection law is already on the books,[15] additional rules, statutes, and authorities are needed

---

10. *Cf. FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security*, FED. TRADE COMM'N 1 (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf [https://perma.cc/3LJV-GYVW] (responding "to Senate Appropriations Committee Report 116-111 accompanying the Financial Services and General Government Appropriations Bill, 2020, directing the [FTC] to 'conduct a comprehensive internal assessment measuring the agency's current efforts related to data privacy and security while separately identifying all resource-based needs of the FTC to improve in these areas'").

11. *Cf. Data Trusts: A New Tool for Data Governance*, ELEMENT AI & NESTA 6, https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf [https://perma.cc/EKG7-SX79] (arguing that private sector self-regulation has failed and data trusts are an effective alternative to legislation for enhanced protection of individual autonomy and privacy).

12. *See, e.g.*, Blayne Haggert, *American Internet, American Platforms, American Values*, CTR. FOR INT'L GOVERNANCE INNOVATION (May 5, 2021), https://www.cigionline.org/articles/american-internet-american-platforms-american-values [https://perma.cc/TWG4-75YW] (describing how U.S. platform firms prioritize free speech, interconnectivity, and interoperability over other values).

13. *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 13-44 (2018) (assessing scholars' varied accounts of the meaning and value of privacy and suggesting conceptions of privacy oriented around the value of trust).

14. Cho et al., *supra* note 6, at 8.

15. For a listing of twenty-three instances of "federal privacy law" governing data or information practices, see Data Protection Act of 2021, S. 2134, 117th Cong. § 2(10)(a)-(w). In the legal sense of digital and online privacy reflected in S. 2134, "privacy" denotes conditions and

to empower the public sector to regulate how companies handle personal information.[16] A new generation of privacy and data-protection laws is evolving in the United States.[17] But promising state and federal initiatives require a hard look to determine whether they go far enough toward addressing the digital-era vulnerabilities of African Americans. The new generation of laws would ideally include provisions specifically geared toward combatting privacy- and data-protection-related racial inequalities enabled by online platforms. A stronger FTC, a freestanding federal data-protection agency, and updated state and federal privacy and data-protection legislation can all potentially help meet contemporary demands for more equitable online-platform governance. How much they can help depends in large part upon whether these measures are pursued boldly and specifically to address the racial-equity challenge.

In Part I of this Essay, I describe the "Black Opticon," a term I coin to denote the complex predicament of African Americans' vulnerabilities to varied forms of discriminatory oversurveillance, exclusion, and fraud—aspects of which are shared by other historically enslaved and subordinated groups in the United States and worldwide.[18] Echoing extant critical and antiracist assessments of digital society, I reference the pervasive calls for improved data-privacy governance, using the lens of race to magnify the consequences for African Americans of what scholars label "surveillance capitalism,"[19] "the darker

---

norms of control over or restricted access to personal information, and the flow of data pertaining to persons. *Cf.* ANITA L. ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY 4-7 (3d ed. 2016) (characterizing informational privacy and five other common senses of privacy found in the law).

16. *Cf.* Taylor Owen, *Introduction: Why Platform Governance?*, *in Models for Platform Governance*, CTR. FOR INT'L GOVERNANCE INNOVATION 3, 3-4 (2019), https://www.cigionline.org/static/documents/documents/Platform-gov-WEB_VERSION.pdf [https://perma.cc/NHC4-YX93] (explaining that because the digital economy touches many aspects of life, issues falling under the platform-governance policy rubric are broad and include data privacy, competition policy, hate-speech enforcement, digital literacy, media policy, and governance of artificial intelligence).

17. *Cf.* Taylor Kay Lively, *US State Privacy Law Tracker*, IAPP (Feb. 10, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/TWZ3-F9RJ] ("State-level momentum for comprehensive privacy bills is at an all-time high."); Muge Fazioglu, *US Federal Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker [https://perma.cc/TXX7-3Q2G] ("[D]ozens of privacy-related bills [have] worked their ways through the halls of Congress.").

18. *See, e.g.*, Nanjala Nyabola, *Platform Governance of Political Speech*, *in Models for Platform Governance*, *supra* note 16, at 63, 63-68 (focusing on Kenyan politics, Cambridge Analytica, and the incitement of ethnic hatred and violence); Sigal Samuel, *China Is Going to Outrageous Lengths to Surveil Its Own Citizens*, ATLANTIC (Aug. 16, 2018), https://www.theatlantic.com/international/archive/2018/08/china-surveillance-technology-muslims/567443 [https://perma.cc/WW97-UUSJ].

19. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 128-75 (2019) (arguing that big data and machine learning allow internet firms to perniciously influence user decisionmaking)); Tressie McMillan Cottom, *Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society*, 6 SOCIO. RACE & ETHNICITY 441, 441 (2020) (arguing that networked capital

narrative of platform capitalism"[20] and "racial capitalism."[21] Privacy advocates repeatedly call for reform to improve online data protections for platform users and the general public who are affected by businesses' data-processing practices.[22] Such reforms also benefit African Americans, of course, to the extent that the interests of African Americans converge with those of the general public. I maintain, however, that generic calls on behalf of all population groups are insufficient to shield the African American community from the Black Opticon. To move from generic to race-conscious reform, I advance a specific set of policy-making imperatives—an African American Online Equity Agenda—to inform legal and institutional initiatives toward ending African Americans' heightened vulnerability to a discriminatory digital society violative of privacy, social equality, and civil rights.[23]

In Part II, I consider whether new and pending U.S. data-privacy initiatives meet the reform imperatives of my African American Online Equity Agenda.[24] I argue that while the Virginia Consumer Data Protection Act is flawed and too new for its full impact to be evaluated,[25] several provisions that could over time reduce race discrimination by private businesses are on the right track. Because the FTC is evidently committed to using its authority to advance the interests of people of color, the U.S. House Energy and Commerce Committee recommendation to allocate a billion dollars to create a new privacy and data-

---

shapes a global racial hierarchy and that public and economic life are privatized). For work further connecting surveillance capitalism to race, see *Surveillance Capitalism*, OPEN MIC, https://www.openmic.org/surveillance-capitalism [https://perma.cc/C39R-RV3V], which observes that "companies' unprecedented, unregulated big-data collection can strip away personal privacy, enable government surveillance, and perpetuate discrimination against poor people and people of color," and that "[t]he surveillance capitalism business model perpetuates racist surveillance, including when tech companies sell products to government agencies."

20. *See* Frank Pasquale, *Two Narratives of Platform Capitalism*, 35 YALE L. & POL'Y REV. 309, 314 (2016).

21. *See* Nancy Leong, *Racial Capitalism*, 126 HARV. L. REV. 2151, 2152 (2013) (defining "racial capitalism" as the "process of deriving social and economic value from the racial identity of another person"); *see also* Angela P. Harris, *Foreword: Racial Capitalism and Law* to HISTORIES OF RACIAL CAPITALISM, at vii, xiii (Destin Jenkins & Dustin Leroy eds., 2021) (asserting that legal engagement with racial capitalism potentially addresses economic inequality, discrimination, algorithmic discrimination, violation of civil rights, and exclusion).

22. *See, e.g.*, *BREAKING: Sen. Gillibrand Introduces U.S. Data Protection Agency Bill*, ELEC. PRIV. INFO. CTR. (June 17, 2021), https://epic.org/2021/06/breaking-sen-gillibrand-introd.html [https://perma.cc/DK39-RAR7] (arguing that Congress's failure to modernize privacy laws imposes "enormous costs on individuals, communities, and American businesses" and urging Congress to enact the Data Protection Act creating a U.S. Data Protection Agency to supplement the inadequate work of the FTC); *see also* Laroia & Brody, *supra* note 2 (emphasizing the importance of preventing data from being used to further marginalize certain groups).

23. When it comes to African Americans, reform proposals include invoking and modernizing civil-rights laws to apply to the digital economy, as well as proposals to improve privacy law and data-protection institutions. I focus on privacy-law and data-protection-institution reforms in this Essay.

24. Privacy law relating to data practices includes common law, state and federal statutes, and regulations and constitutional provisions that prescribe, prohibit, incentivize, or reward conditions that limit access to or sharing of information about persons, such as strict adherence to fair-information practices, anonymization, differential privacy, and cybersecurity.

25. VA. CODE ANN. §§ 59.1-575 to -585 (2021) (effective Jan. 1, 2023).

protection bureau within the Commission is on point for reducing online fraud and deception targeting African Americans.[26] Finally, though unlikely to be passed by Congress in the very near term, privacy legislation introduced by Senator Kristen Gillibrand in 2021 is remarkably equity conscious, setting the bar high for future federal legislation.[27]

I conclude that although we must welcome these major reforms and proposals for advancing online equity, privacy, and consumer-data protection, grounds for concern remain when reforms are assessed against imperatives for specifically combatting African American disadvantage. Whether and to what extent contemplated legal and institutional reforms would free African Americans from the Black Opticon remains an open question. However, the current era of privacy and data-protection reform presents a paramount opportunity to shape law and legal institutions that will better serve African Americans' platform-governance-related interests no less than, and along with, the interests of others.

## i. the black opticon: african americans' disparate online vulnerability

African Americans dwell under the attentive eye of a Black Opticon, a threefold system of societal disadvantage comprised of discriminatory oversurveillance (the panopticon),[28] exclusion (the ban-opticon),[29] and

---

**26.** *See* FED. TRADE COMM'N, *supra* note 9, at 47 ("The FTC is committed to serving communities of color through vigorous law enforcement actions, meaningful community engagement and dialogue, and the pursuit of insightful research."); *see also* H. COMM. ON ENERGY & COM., 117TH CONG., LEGISLATIVE RECOMMENDATIONS RELATING TO FTC PRIVACY ENFORCEMENT 1 (Comm. Print 2021) (recommending billion-dollar appropriation to FTC for privacy enforcement).

**27.** *See* Data Protection Act of 2021, S. 2134, 117th Cong.

**28.** JEREMY BENTHAM, *Panopticon, or, the Inspection House*, *in* THE PANOPTICON WRITINGS 10, 11 (Miran Božovič ed., Verso 1995) (1791) (describing a design for institutions of close surveillance, such as schools, prisons, hospitals, and asylums, whereby inspectors see without being seen and inmates always feel as if under actual or possible inspection). A panoptic society enables personal data to be deployed for surveillant social control. *Cf.* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 170-71 (1975) (arguing that hierarchical observation in the panopticon "coerces by means of observation; an apparatus in which the techniques that make it possible to see induce effects of power"). It is interesting to note that surveillant societies rely on sensorial modes in addition to vision. Offline, the law-enforcement sniffer dog relies on smell to detect drugs and explosives; the wiretap relies on sound. *See* Irus Braverman, *Passing the Sniff Test: Police Dogs as Surveillance Technology*, 61 BUFF. L. REV. 81 (2013) (examining drug-sniffing dogs as a form of surveillance technology); Tony Wu, Justin Chung, James Yamat & Jessica Richman, *The Ethics (or Not) of Massive Government Surveillance*, STAN. COMPUT. SCI., https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_wiretapping.html [https://perma.cc/D3JP-WY86] (providing background on wiretapping technology).

**29.** A play on panopticon, "ban-opticon," is a term derived from Didier Bigo, *Globalized (In)Security: The Field and the Ban-opticon*, *in* TERROR, INSECURITY AND LIBERTY: ILLIBERAL PRACTICES OF LIBERAL REGIMES AFTER 9/11, at 10, 32-33 (Didier Bigo & Anastassia Tsoukala eds.,

predation (the con-opticon).[30] This disadvantage—propelled by algorithms and machine-learning technologies that are potentially unfair and perpetuate group bias—is inimical to data privacy and an ideal of data processing that respects the data subject's claim to human dignity and equality. Structural racism renders African Americans especially vulnerable to disparities and disadvantages online.[31] Highlighting the problem of algorithmic bias, Dominique Harrison asserted that "Black and Brown people are stripped of equitable opportunities in housing, schools, loans, and employment because of biased data."[32] As Harrison's observations attest, my Black Opticon metaphor—denoting the ways Black people and their data can be visually observed and otherwise paid attention to online—encapsulates literal aspects of the urgent privacy and data-protection problem facing African Americans.

African Americans are active users of online platforms. Although roughly thirty percent of Black homes lack high-speed internet access and seventeen percent lack a home computer,[33] Black Americans are well-represented among the 300 to 400 million users of Twitter and the billions of daily users of Meta (previously known as Facebook) platforms.[34] African Americans accounted for nearly one-tenth of all Amazon retail spending in the United States in 2020.[35] As the digital divide is closing among younger Americans,[36] commentators extol

---

2008). The ban-optic society enables uses of personal data that target marginalized groups for opportunity exclusion, pushing their legitimate interests to the wayside, beyond civil society's sightlines.

30. Continuing the Benthamite wordplay, I introduce here for the first time the term "con-opticon." The con-optic society enables financial predation, exploiting marginalized people's vulnerability to con-jobs of consumer scams, fraud, and deceit.

31. *Cf.* SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 4 (2018) (underscoring "the structural ways that racism and sexism are fundamental" to automated decision-making that masks and deepens social inequality).

32. Dominique Harrison, *Civil Rights Violations in the Face of Technological Change*, ASPEN INST. (Oct. 22, 2020), https://www.aspeninstitute.org/blog-posts/civil-rights-violations-in-the-face-of-technological-change [https://perma.cc/35KC-QP6G].

33. *See Expand Internet Access Among Black Households*, JOINT CTR. FOR POL. & ECON. STUD. (Aug. 4, 2020), https://jointcenter.org/expand-internet-access-among-black-households [https://perma.cc/RB7G-AFWK].

34. *See* Aaron Smith, *Detailed Demographic Tables*, PEW RSCH. CTR. (Jan. 6, 2014), https://www.pewresearch.org/internet/2014/01/06/detailed-demographic-tables [https://perma.cc/34ZS-WB66]; *see also* ANDRÉ BROCK JR., DISTRIBUTED BLACKNESS: AFRICAN AMERICAN CYBERCULTURES 81 (2020) (describing the growth of "Black Twitter" as a place for "shar[ing] Black cultural commonplaces, [] build[ing] social affinities," and often intragroup social-policing); *cf. Facebook - Statistics and Facts*, STATISTA (Nov. 28, 2021), https://www.statista.com/topics/751/facebook/#dossierKeyfigures [https://perma.cc/M3GV-TL3W] (asserting that there are 2.8 billion daily users of all Facebook-owned platforms).

35. D. Tighe, *Amazon Share of Consumer Retail Spending in the U.S. in 2020, by Race and Ethnicity*, STATISTA (Feb. 15, 2021), https://www.statista.com/statistics/1201884/share-consumer-spending-amazon-united-states-by-race [https://perma.cc/WCL8-NSTU].

36. Pew Research reports that social-media usage in the United States is relatively consistent across race and ethnicity, though the choice of *which* social-media platforms to use most frequently varies by race. *See* Jens Manuel Krogstad, *Social Media Preferences Vary by Race and Ethnicity*, PEW RSCH. CTR. (Feb. 3, 2015), https://www.pewresearch.org/fact-tank/2015/02/03/social-media-preferences-vary-by-race-and-ethnicity [https://perma.cc/3XZ7-A46Q]. Furthermore, Black people are often among the most likely to use social-media platforms for social activism, with "younger Black users being more likely to do these things

a vibrant African American "cyberculture" of everyday life.[37] Black people's recent civil-rights strategies include racial-justice advocacy that is digitally mediated.[38] While Black users and designers of online technology were once a faint presence in popular and academic discussions of the digital age, today, "Black digital practice has become hypervisible to . . . the world through . . . Black cultural aesthetics . . . and social media activism."[39] On a more mundane level, Black Americans turn to internet platforms for access to housing, education, business, employment, loans, government services, health services, and recreational opportunities.[40]

---

than older Black users." Brooke Auxier, *Social Media Continue to Be Important Political Outlets for Black Americans*, PEW RSCH. CTR. (Dec. 11, 2020), https://www.pewresearch.org/fact-tank/2020/12/11/social-media-continue-to-be-important-political-outlets-for-black-americans [https://perma.cc/3J8M-P9GU]. The digital divide today is therefore a gap in quality and amount of time spent online, not a gap in access to internet. *See* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 140 (2017) (suggesting that what distinguishes the wealthy from the poor may no longer simply be access but the quality of access).

37. BROCK, *supra* note 34, at 6 (describing "the ways Black folk use the internet as a space to extol the joys and pains of everyday life—the hair tutorials, the dance videos, the tweetstorms, and more").

38. *See* MCILWAIN, *supra* note 3 (detailing African Americans' efforts to harness technological platforms for personal, communal, and political interests); ALLISSA V. RICHARDSON, BEARING WITNESS WHILE BLACK: AFRICAN AMERICANS, SMARTPHONES, AND THE NEW PROTEST #JOURNALISM (2020) (detailing tech-facilitated anti-police-brutality activism and protest journalism in the Black community). Research from the Pew Research Center concludes that social media is an important political outlet for African Americans. *See* Auxier, *supra* note 36; *see also Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media [https://perma.cc/4X8E-YS7K] (analyzing social-media use generally by race and other demographics).

39. BROCK, *supra* note 34, at 17.

40. *Cf.* Michael Chui, Brian Gregg, Sajal Kohli & Shelley Stewart III, *A $300 Billion Opportunity: Serving the Emerging Black American Consumer*, MCKINSEY Q. (Aug. 6, 2021), https://www.mckinsey.com/featured-insights/diversity-and-inclusion/a-300-billion-dollar-opportunity-serving-the-emerging-black-american-consumer [https://perma.cc/V4J3-C5LP] ("Black consumers are actually more likely than others to participate in e-commerce, despite disparities in broadband connections and computer availability."); *see also* Aaron Smith, *Government Online: The Internet Gives Citizens New Paths to Government Services and Information*, PEW RSCH. CTR. (Apr. 27, 2010) ("African Americans and Latinos are just as likely as whites to use tools such as blogs, social networking sites and online video to keep up with the workings of government."). *But see* Jamie M. Lewis, *Differences in Accessing Online Health Resources by Race and Ethnicity*, U.S. CENSUS BUREAU (Apr. 27, 2017), https://www.census.gov/newsroom/blogs/research-matters/2017/04/accessing-online-resources-by-race-ethnicity.html [https://perma.cc/72N6-A6RR] ("We find that race matters for use of online health resources . . . . People who are black, Asian and Hispanic are less likely than non-Hispanic white people to research health information online. Black people are also less likely than non-Hispanic white people to go online to communicate with a doctor or check health records."); Sara Atske & Andrew Perrin, *Home Broadband Adoption, Computer Ownership Vary by Race, Ethnicity in the U.S.*, PEW RSCH. CTR. (July 16, 2021), https://www.pewresearch.org/fact-tank/2021/07/16/home-broadband-adoption-computer-ownership-vary-by-race-ethnicity-in-the-u-s [https://perma.cc/GSV3-5AUB ] (showing that Black people are less likely than white people to have a home computer but

It may appear that African American platform users, like other groups of users, are not overly concerned with privacy and data protection because of their seeming readiness to give away identifiable personal information.[41] While some consumers indeed undervalue privacy,[42] privacy-abandonment behaviors may not signal genuine indifference to privacy for several reasons.[43] Low-income African Americans may decline privacy protections, such as smartphone encryption, due to prohibitive costs of data-secure devices and services.[44] Some consumers trust that Big Tech is sufficiently caring, comprehensively regulated, and responsive to closing gaps in privacy protection.[45] Typical consumers experience corporate data practices as a black box.[46] Terms of service and privacy policies, while available online, are lengthy, technical, and complex.[47] Educated and uneducated users are poorly informed about the implications of joining a platform, and once on board a platform, stepping off to recover a

---

equally or more likely to have a smartphone and/or tablet device; but "63% of Black adults—compared with 49% of White adults—say not having high-speed internet puts people at a major disadvantage when it comes to connecting with doctors or other medical professionals"). Exemplifying Black people's use of the internet for recreation, see Wellington Webb, *Internet Gambling Harmful to Minorities*, HILL (Sept. 11, 2014), https://thehill.com/opinion/op-ed/217316-internet-gambling-harmful-to-minorities [https://perma.cc/DR9R-CE48] ("Pew Internet Research suggests that minority communities are uniquely susceptible to the threat posed by 24/7 access to Internet gambling, finding that African Americans and Latinos are more likely than whites to both own a smartphone and count on those phones for uses other than making calls.").

41. *See* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1022 (2013).

42. ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 6-11 (2011) (arguing that in a just, free society, privacy-protecting nudges and laws are justified paternalistically even though the public may be indifferent or hostile to privacy).

43. In a subtle analysis of the "allure and illusion" of "notice and consent" to online data processing, Robert H. Sloan and Richard Warner distinguish consent from acquiescence and acceptance, and they describe processes of normative acculturation that they say explain consumers' relationship to privacy values and online surveillance. *See* ROBERT H. SLOAN & RICHARD WARNER, THE PRIVACY FIX: HOW TO PRESERVE PRIVACY IN THE ONSLAUGHT OF SURVEILLANCE 103-16 (2021).

44. *Cf. Buying a Smart Phone on the Cheap? Privacy Might Be the Price You Have to Pay*, PRIV. INT'L (Sept. 20, 2019), https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay [https://perma.cc/FR63-VL8V] (reporting on research showing that inexpensive smartphones sometimes come with preinstalled, undeletable apps that leak user data)).

45. *Cf.* Patrick Seitz, *Survey Reveals Which Tech Companies Consumers Trust the Most*, INV'S. BUS. DAILY (Aug. 2, 2021, 8:00 AM ET), https://www.investors.com/news/technology/tech-stocks-survey-reveals-which-tech-companies-consumers-trust-the-most [https://perma.cc/MM9L-8P83] (revealing a high level of consumer trust in Amazon); *see also* Will Johnson, *Survey: Americans Think Big Tech Isn't So Bad After All*, HARRIS POLL (Dec. 10, 2020), https://theharrispoll.com/survey-americans-think-big-tech-isnt-so-bad-after-all [https://perma.cc/S245-S4G3] (reporting that polling data suggest consumer comfort with and trust in platform companies used in daily life). *But see* Brooke Auxier, *How Americans See U.S. Tech Companies as Government Scrutiny Increases*, PEW RSCH. CTR. (Oct. 27, 2020), https://www.pewresearch.org/fact-tank/2020/10/27/how-americans-see-u-s-tech-companies-as-government-scrutiny-increases [https://perma.cc/4GZD-SDHU] (reporting that the majority of people polled view tech as harmful and requiring more regulation, while a minority think existing regulation is adequate).

46. *See* PASQUALE, *supra* note 4, at 3 ("[T]racked ever more closely by firms and government, we have no clear idea just how far much of this information can travel, how it is used, or its consequences.").

47. *Id*. at 143-45.

semblance of control over data can sever important channels of communications and relationships.[48]

I believe many African Americans do care about their data privacy, and that their understanding of the many ways it is unprotected is growing. The remainder of this Part describes the three constitutive elements of the Black Opticon of African American experience: (1) discriminatory oversurveillance (the panopticon), (2) discriminatory exclusion (the ban-opticon), and (3) discriminatory predation (the con-opticon). In so doing, it illustrates how attentive eyes within American society misperceive African Americans through warped lenses of racial discrimination.

### *A. Discriminatory Oversurveillance*

Elements of the Black Opticon have been recognized for decades. In fact, since the dawn of the computer age, wary privacy scholars have emphasized that watching and monitoring individuals with the aid of technology threatens privacy—both for its tendency to chill and control behavior, and for its potential to efficiently reveal and disseminate intimate, personal, incriminating, and sensitive information. For example, Alan Westin's 1964 treatise, *Privacy and Freedom*, among the most influential law-related privacy studies of all time, noted the special susceptibility of African Americans to the panoptic threat.[49] According to Westin, privacy denotes a certain claim that all people make for self-determination: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[50] Distinguishing physical, psychological, and data surveillance, Westin explicitly mentioned African Americans in relation to concerns about covert physical surveillance and discrimination by segregationists within a white power structure.[51] Arthur R. Miller raised political surveillance as a privacy problem facing African Americans in his landmark 1971 *Assault on Privacy*.[52] And a more obscure early book devoted to privacy in America, Michael F. Mayer's 1972 *Rights of Privacy*,[53] decried the unlawful wiretapping surveillance of Martin Luther King Jr. that was revealed in the trial of Cassius Clay (Muhammed Ali).[54] Mayer devoted a short chapter to the

---

48. Pasquale, *supra* note 41, at 1014-16.

49. ALAN F. WESTIN, PRIVACY AND FREEDOM 115 (1967).

50. *Id.* at 7.

51. *Id.* at 68, 115 ("The struggle over segregation and civil rights has prompted considerable electronic surveillance of Negro and white integrationist groups by some private segregationist organizations in southern states.").

52. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 200-02 (1971).

53. MICHAEL F. MAYER, RIGHTS OF PRIVACY (1972).

54. *Id.* at 87.

oversurveillance of the poor dependent on government housing and other benefits,[55] foreshadowing Khiara M. Bridges's work on privacy and poverty.[56]

Twitter, Facebook, Instagram, and nine other social-media platforms came under attack in 2016 for providing location-analytics software company Geofeedia with access to location data and other social-media information[57]—an illustration of platform-related oversurveillance. According to an American Civil Liberties Union report that year, police departments used software purchased from Geofeedia that relied on social-media posts and facial-recognition technology to identify protesters.[58] For example, following the Black Lives Matter (BLM) protests sparked by the death of African American Freddie Gray while in police custody, Baltimore police reportedly used Geofeedia software to track down and arrest peaceful protesters with outstanding warrants.[59] Police deliberately focused arrests within the majority Black community of Sandtown-Winchester, the precinct where Freddie Gray was apprehended and killed.[60] Geofeedia continued to market its services as a way to track BLM protesters at a time when the FBI was a Geofeedia client and an FBI report indicated that a so-called "Black Identity Extremist" movement

---

55. *Id.* at 54-60.

56. BRIDGES, *supra* note 36, at 10 (observing that poor mothers in need of government welfare do not have privacy rights and are expected to grant access to their lives, bodies, and information, resulting in a loss of dignity and autonomy).

57. *See* Sam Levin, *ACLU Finds Social Media Sites Gave Data to Company Tracking Black Protesters*, GUARDIAN (Oct. 11, 2016, 4:07 PM EDT), https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter [https://perma.cc/FVC5-Y44L] (explaining that Facebook's "Topic Feed API" contains a feed of public posts organized around specific hashtags, events, or places and includes location data); Jonah Engel Bromwich, Daniel Victor & Mike Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html [https://perma.cc/B76D-PNSP].

58. *See* Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU (Oct. 11, 2016), https://www.aclu.org/blog/privacy-technology/internet-privacy/facebook-instagram-and-twitter-provided-data-access [https://perma.cc/3WP3-6PA4].

59. *See id.* (stating that the ACLU is concerned about social media's lack of robust or properly enforced antisurveillance policies); *see also* Ethan McLeod, *Police Arrested Freddie Gray Protesters Last Year by Surveilling Social Media, Baltimore Fishbowl*, BALT. FISHBOWL (Oct. 12, 2016), https://baltimorefishbowl.com/stories/police-arrested-freddie-gray-protesters-last-year-surveilling-social-media [https://perma.cc/RQ7V-R5KP] ("Officers were able to single out and arrest protesters with outstanding warrants during the Freddie Gray riots with help from a social media monitoring tool, the ACLU has found.").

60. *Baltimore Country Police Department Partners and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, GEOFEEDIA, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf [https://perma.cc/D238-85TZ] (describing social-media surveillance and facial-recognition targeting the community "where Gray had been arrested"). Freddie Gray lived, was arrested, and died in the Sandtown-Winchester community located within the Western District precinct of the Baltimore police. *Cf.* Dewayne Wickham, *Focus on Freddie Gray's Neighborhood*, USA TODAY (May 5, 2015, 7:15 PM ET), https://www.usatoday.com/story/opinion/2015/05/04/freddie-gray-neighborhood-wickham-column/26834967 [https://perma.cc/5BFJ-5NHV] (describing where Gray lives, was arrested and died); *Western District*, BALT. POLICE DEP'T, https://www.baltimorepolice.org/find-my-district/western-district [https://perma.cc/S7ZS-UEDZ] (showing that the Western District of Baltimore police includes Sandtown-Winchester).

would be a target of surveillance.[61] As imprecisely defined by the FBI, the label "Black Identity Extremist" could be affixed to an activist who merely protested police brutality.[62] Fortunately for African Americans and all social-media users, Twitter, Facebook, and Instagram discontinued sharing location data and social-media feeds with Geofeedia following public backlash.[63] But panoptic concerns about platforms and privacy will remain so long as efforts to subject Black people to special levels of efficient social control persist.[64]

Today, government and nongovernmental surveillance practices and technologies of all kinds disparately impact communities of color.[65] The Geofeedia example demonstrates how data sharing and disclosures by digital platforms can have far-reaching inequitable consequences for African

---

61. Mana Azarmi, *The FBI's "Black Identity Extremists" Report and the Surveillance Reform Debate*, CTR. FOR DEMOCRACY & TECH. (Dec. 18, 2017), https://cdt.org/insights/the-fbis-black-identity-extremists-report-and-the-surveillance-reform-debate [https://perma.cc/B5TP-3XRY]; Ally Marotti, *Chicago Police Used Geofeedia, the TweetDeck for Cops Under Fire from ACLU*, CHI. TRIB. (Oct. 13, 2016, 2:30 PM), https://www.chicagotribune.com/business/blue-sky/ct-geofeedia-police-surveillance-reports-bsi-20161013-story.html [https://perma.cc/AWW3-AGHH] ("The Intercept reported that In-Q-Tel, the CIA's venture firm, has invested in Geofeedia. The FBI has also used the platform, says a separate document that fueled stories by The Daily Dot.").

62. 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 [https://perma.cc/Q7HB-FBCE].

63. Noting the discontinuance, see, for example, Brandon Russell, *Can Facebook and Twitter Stop Social Media Surveillance?*, VERGE (Oct. 12, 2016), https://www.theverge.com/2016/10/12/13257080/police-surveillance-facebook-twitter-instagram-geofeedia [https://perma.cc/6REC-VKMC].

64. Geofeedia was not the end of the story of the panoptic threat of oversurveillance. *See* Dell Cameron, *Dozens of Police-Spying Tools Remain After Facebook, Twitter Crack Down on Geofeedia*, DAILY DOT (Oct. 11, 2016), https://www.dailydot.com/irl/geofeedia-twitter-facebook-instagram-social-media-surveillance [https://perma.cc/3U5T-G225] (reporting that law-enforcement surveillance is aided by the products of specialty firms); *cf.* WILLIAM I. ROBINSON, *Savage Inequalities: The Imperative of Social Control*, *in* THE GLOBAL POLICE STATE 41, 66 (2020) (providing a neomarxist analysis of why dominant groups will confront the escalating challenge of social control in the face of massive inequalities and social polarization). Michel Foucault's famous insights concerning panoptic surveillance and the efficiency of the constraint that comes with the power to place human subjects under observation and the threat of observation are also relevant here. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 202 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977) ("[I]t is not necessary to use force to constrain the convict to good behaviour, the madman to calm, the worker to work, the schoolboy to application, the patient to the observation of the regulations. Bentham was surprised that panoptic institutions could be so light: there were no more bars, no more chains, no more heavy locks; all that was needed was that the separations should be clear and the openings well arranged. The heaviness of the old 'houses of security', with their fortresslike architecture, could be replaced by the simple, economic geometry of a 'house of certainty'. The efficiency of power, its constraining force have, in a sense, passed over to the other side – to the side of its surface of application.").

65. *See, e.g.*, TED Radio Hour, *Joy Buolamwini: How Do Biased Algorithms Damage Marginalized Communities*, NPR (Feb. 26, 2021, 10:13 AM ET), https://www.npr.org/2021/02/26/971506520/joy-buolamwini-how-do-biased-algorithms-damage-marginalized-communities [https://perma.cc/2FAH-FHLU].

Americans. The business of providing platform users' location data and social-media posts to third parties, including law enforcement, without express consent or transparency is aptly perceived by platform critics as violating users' legitimate information-privacy interests.[66] Data-privacy interests are implicated whenever consumer data collected or shared for one purpose is used for other purposes without consent and transparency. A panoptic threat grows as the extent, frequency, and pervasiveness of information gathering through surveillance grows. The Black Opticon exists—and has long existed—inasmuch as wrongful discrimination and bias persistently focus panoptic surveillance on African Americans, leading to oversurveillance.[67] Location tracking, the related use of facial-recognition tools, and targeted surveillance of groups and protestors exercising their fundamental rights and freedoms are paramount data-privacy practices disproportionally impacting African Americans.

### *B. Discriminatory Exclusion*

I now turn to another feature of the Black Opticon, namely, targeting Black people for exclusion from beneficial opportunities on the basis of race. Discriminatory exclusion requires obtaining information identifying a person as African American.

Such information is not hard to come by. In the 1950s, a brick-and-mortar business could obtain race information from the City Directory. In Atlanta, Georgia, for example, white-only businesses wishing to avoid soliciting business from African Americans could use race information published in the 1951 City Directory.[68] The directory designated people known to be Black with a "c" for

---

66. *See, e.g.*, Letter from Color of Change, ACLU of California & Ctr. for Media Just. to Twitter (Oct. 10, 2016), https://www.aclunc.org/sites/default/files/20161010_ACLU_CMJ_Color_of_Change_Joint_letter_Twitter.pdf [https://perma.cc/TR94-EUYX] ("Twitter should not provide user data access to developers who have law enforcement clients and allow their product to be used for surveillance, including the monitoring of information about the political, religious, social views, racial background, locations, associations or activities of any individual or group of individuals."); *id.* ( "Twitter should adopt clear and transparent public policies that prohibit developers from using Twitter data to facilitate surveillance and publicly explain these policies, how they will be enforced, and the consequences of such violations."); Letter from Color of Change, ACLU of California & Ctr. for Media Just. to Facebook and Instagram (Oct. 10, 2016), https://www.aclunc.org/sites/default/files/20161010_ACLU_CMJ_Color_of_Change_Joint_letter_Facebook_Instagram.pdf [https://perma.cc/N7RB-RMVQ] ( "Facebook and Instagram should not provide user data access to developers who have law enforcement clients and allow their product to be used for surveillance, including the monitoring of information about the political, religious, social views, racial background, locations, associations or activities of any individual or group of individuals."); *id.* ("Facebook and Instagram should adopt clear and transparent public policies that prohibit developers from using Facebook and Instagram data to facilitate surveillance and publicly explain these policies, how they will be enforced, and the consequences of such violations." ); *cf.* Nick Doty & Eric Wild, Geolocation Privacy and Application Platforms (Nov. 2, 2010) (unpublished manuscript), https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.423.4322&rep=rep1&type=pdf [https://perma.cc/C2XG-TBFM] (describing the privacy issues raised by geolocation capabilities of common devices).

67. *See supra* notes 49-53 (citing privacy scholars writing in the 1960s and 1970s who observed that Black people are targeted for surveillance).

68. The 1951 Atlanta, Georgia City Directory listed such details as a person's race, occupation, marital status, and street address, suggesting that business and consumer users of the

colored.[69] The Directory also included information from which race might be deduced due to segregation in housing and employment, such as the entrant's street address and employment.[70] African Americans who did not wish to be discriminated against might have aspired to keep their race private. But in the old South, neither civility norms nor laws protected race information from disclosure.

Today, similar information can be used to identify a person as African American. For example, residential addresses continue to serve as racial proxies.[71] And even something as basic as a person's name can reveal their race. These racial proxies then facilitate discriminatory exclusion. For example, Dr. LaTanya Sweeney, Harvard professor and former Chief Technology Officer at the FTC, uncovered that when she typed her name into Google an advertisement for InstaCheckmate.com captioned "LaTanya Sweeney Arrested?" popped up.[72] When she searched for the more ethnically ambiguous "Tanya Smith," the arrest-association advertisement disappeared. As Sweeney's work demonstrates, biased machine learning can lead search engines to presume that names that "sound Black" belong to those whom others should suspect and pay to investigate.[73]

Online businesses have the capacity to discriminate and exclude on the basis of race, just as brick-and-mortar businesses have done. Discriminatory exclusion by government and in places of public accommodation is both a civil-rights and a privacy issue. In the 1960s and 1970s, legal commentators began to frame uses of information about race to discriminate and exclude Black people from opportunity as among the nation's information-privacy problems. For example, Miller pointed out in *Assault on Privacy* that psychological testing, which excluded some minorities from employment and school admissions,

---

directories would wish to know or confirm those details. (It was by viewing my mother's entry in the City Directory accessed via Ancestry.com that I learned that as a teenager she had worked in the kitchen of a popular restaurant catering to white women and that my grandfather, listed as "c" for colored, worked for an electrical supply company.) *See* CITY DIRECTORY, ATLANTA, GA. 328-29 (1951), https://www.ancestry.com/imageviewer/collections/2469/images/12208671?backlabel=ReturnSearchResults&queryId=0a94257bc266a5956c0f3c5e25a894ed&pId=1246072253 [https://perma.cc/NPM2-JJK4]; *cf.* Lynn Peeples, *Death of the Directory, When Was the Last Time You Opened a Phone Book?*, SCI. AM. (Aug. 27, 2009), https://blogs.scientificamerican.com/news-blog/death-of-the-directory-when-was-the-2009-08-27 [https://perma.cc/6RZA-6MVE] ("Southern cities typically printed two books—numbers were segregated by race, like everything else in society.").

69. See, for example, CITY DIRECTORY, *supra* note 68, at 329, listing my grandfather, Emizi Cloud, as "c."

70. *See* CITY DIRECTORY, *supra* note 70.

71. *Cf.* Anya E.R. Prince & Daniel Schwartz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1262 (2020) ("The usefulness to firms of refusing to serve redlined geographic regions was that it allowed them to covertly achieve their discriminatory aims.").

72. PASQUALE, *supra* note 4, at 39.

73. *Id.* at 39.

required test takers to respond to invasive personal questions.[74] In the 1970s, when unfair credit practices could easily exclude people of color from lending opportunities, policy makers linked fair credit goals to consumer-information privacy.[75] Privacy rights were understood to include the right to withhold information, to restrict sharing with third parties, and to access and correct credit-reporting information.[76]

The forms of racism and inequality of opportunity that policy makers recognized in the 1970s permeate today's digital sphere, in the exclusionary practices of the sort Didier Bigo would term ban-optic.[77] Discriminatory practices (i.e., those that rely on racialized sorting by humans and machines that reinforce racism and deny equal access to services and opportunities[78]) thrive on online platforms. Platforms have come under attack for targeted advertising that discriminates against consumers of color with respect to housing, credit, and services, for hosting racially biased advertisements, and for facilitating unequal and discriminatory access to ridesharing and vacation rentals.[79]

Nonconsensual and discriminatory uses of personal information, like other unauthorized use and disclosure of personal information, should be understood as information-privacy violations.[80] For a time, advertisers on Facebook were able to select which Facebook users could and could not see their

---

**74.** *Cf.* MILLER, *supra* note 52, at 90-105 (describing state surveillance through IQ and ability testing); *id.* at 91-92 (explaining that the issue has arisen of "whether testing discriminates against blacks and other disadvantaged groups"); *id.* at 93 ("[A]chievement, aptitude, and intelligence test . . . suggest privacy problems that are somewhat more subtle than . . . blatantly intrusive interrogations."). *See generally* WESTIN, *supra* note 49, at 242-78 (describing privacy concerns relating to prying personality testing); *id.* at 257 (noting that the Illinois Fair Employment Practices Commission found that a Motorola company "ability" test discriminated against an African American applicant).

**75.** *See* MILLER, *supra* note 52, at 67-90.

**76.** Fair-information-practice principles were introduced in the early 1970s. *See* Gellman, *supra* note 8 (manuscript at 1).

**77.** *See* Bigo, *supra* note 29, at 10, 32-33.

**78.** *See* OSCAR H. GANDY JR., THE PANOPTIC SORT 15-17 (2d ed. 2021) (describing privacy implications of assigning people to groups via "sorting" to make manipulation easier).

**79.** *See, e.g.*, Jennifer Eberhardt, *Can AirBnB Train Hosts Not to Be Racists?*, DAILY BEAST (June 12, 2019, 12:47 PM ET), https://www.thedailybeast.com/can-airbnb-train-hosts-not-to-be-racists [https://perma.cc/29TB-G64S]; Dave Lee, *AirBnB Racism Claim: African-Americans 'Less Likely to Get Rooms'*, BBC (Dec. 12, 2015), https://www.bbc.com/news/technology-35077448 [https://perma.cc/36PE-64GG]; Edward Ongweso Jr., *Uber Is Getting Sued Over Its Allegedly Racist Ratings System*, VICE (Oct. 27, 2020, 2:26 PM), https://www.vice.com/en/article/v7mg89/uber-is-getting-sued-over-its-allegedly-racist-ratings-system [https://perma.cc/YE77-Y6DB]; Andrew Kersley, *Couriers Say Uber's 'Racist' Facial Identification Tech Got Them Fired*, WIRED (Jan. 3, 2021, 6:00 AM), https://www.wired.co.uk/article/uber-eats-couriers-facial-recognition [https://perma.cc/6DU4-Z3S6].

**80.** I note that the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x (2018), is considered one of the first federal *privacy* statutes because key provisions restricted "consumer reporting agencies" from sharing with third parties the sensitive information they otherwise legitimately collected. *See Fair Credit Reporting Act*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act [https://perma.cc/3GN3-BZZG] ("Information in a consumer report cannot be provided to anyone who does not have a purpose specified in the Act."). Other provisions give consumers rights to have disputes investigated, information corrected, adverse decisions disclosed and identity theft protection. *Id.*

advertisements by race.[81] The ability to target sectors of the market meant that African Americans could be excluded from commercial opportunities on the basis of their race alone. In November 2017, after Facebook claimed to have devised a system that would recognize and not post discriminatory housing advertisements, journalists at ProPublica were able to purchase housing advertisements that excluded classes protected by the Fair Housing Act, including African American users and users interested in wheelchair ramps.[82] A representative from Facebook explained ProPublica's racially discriminatory housing advertisements as a technical failure.[83] In 2019, showing that some data-privacy problems can and should also be framed as civil-rights violations,[84] the U.S. Department of Housing and Urban Development charged Facebook with violating the Fair Housing Act by selling advertisements that discriminate against protected classes.[85] Facebook's current policies prohibit discrimination based on race.[86]

---

**81.** *See generally* Sheryl Sandberg, *Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising*, META (Mar. 19, 2019), https://about.fb.com/news/2019/03/protecting-against-discrimination-in-ads [https://perma.cc/WCF7-HZQA] ("Last year, one of the US's top housing civil rights organizations, the National Fair Housing Alliance (NFHA), as well as the American Civil Liberties Union (ACLU), the Communication Workers of America (CWA) and other private parties, filed litigation against us, saying that we need to build stronger protections against abuse. Civil rights leaders and experts—including members of the Congressional Black Caucus, the Congressional Hispanic Caucus, the Congressional Asian Pacific American Caucus and Laura Murphy, the highly respected civil rights leader who is overseeing the Facebook civil rights audit—have also raised valid concerns about this issue.").

**82.** Julia Angwin & Ariana Tobin, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, PROPUBLICA (Nov. 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin [https://perma.cc/K3YH-9MV4] ("After ProPublica revealed last year that Facebook advertisers could target housing ads to whites only, the company announced it had built a system to spot and reject discriminatory ads. We retested and found major omissions.").

**83.** *Id.* (reporting that Facebook responded to ProPublica by saying "[t]his was a failure in our enforcement and we're disappointed that we fell short of our commitments").

**84.** *See* Dominique Harrison, *Civil Rights Violations in the Face of Technological Change*, ASPEN INST. (Oct. 22, 2020), https://www.aspeninstitute.org/blog-posts/civil-rights-violations-in-the-face-of-technological-change [https://perma.cc/G8VF-27V4] ("[C]ommunities of color face a battle to uphold civil rights that have been abridged through online platforms."). While it is beyond the scope of this Essay, a close comparison of the strengths and weakness of civil-rights and privacy-rights strategies is warranted.

**85.** *Hud Charges Facebook with Housing Discrimination over Company's Targeted Advertising Practices*, U.S. DEP'T HOUS. & URB. DEV. (Mar. 28, 2019), https://archives.hud.gov/news/2019/pr19-035.cfm [https://perma.cc/S5CH-QQYD].

**86.** *Cf. Review Compliance for Facebook's Non-Discrimination Policy*, META FOR BUS.: META BUS. HELP CTR., https://www.facebook.com/business/help/136164207100893 [https://perma.cc/8Q7Q-JNHF] ("Our Advertising Policies prohibit advertisers from using our ads products to discriminate against individuals or groups of people. Ads are discriminatory when they deny opportunities to individuals or groups of people based on certain personal attributes such as race, ethnicity, national origin, religion, age, sex, sexual orientation, gender identity, family/marital status, disability or medical or genetic condition. Anytime you run Facebook ads, you're already agreeing to follow our non-discrimination policy.").

### *C. Discriminatory Predation*

Personal data of people of color are also gathered and used to induce purchases and contracts through con jobs, scams, lies, and trickery. Discriminatory predation describes the use of communities of color's data to lure them into making exploitative agreements and purchases. This feature of the Black Opticon searches out and targets vulnerable African Americans online and offline for con-job inclusion. Predatory surveillance is the flip side of the exclusionary-surveillance coin.

Discriminatory predation makes consumer goods such as automobiles and for-profit education available, but at excessively high costs.[87] Predation includes selling and marketing products that do not work,[88] extending payday loans with exploitative terms,[89] selling products such as magazines that are never delivered,[90] and presenting illusory money-making schemes to populations desperate for ways to earn a better living.[91] The FTC has gone after wrongdoers for the practice of targeting low-income individuals.[92] The agency has noted that Native Americans, Latinos, African Americans, immigrants, and inmates and their families are disproportionately impacted by fraud.[93] These populations are lured through false, unfair, or fraudulent online and offline advertising, marketing, and promotions for consumer goods, medical products, government services, education, employment, and business opportunities.[94]

Recent litigation focused on the company MyLife.com.[95] MyLife.com is an online enterprise that sells profiles of individuals, marketed for purposes including housing, credit, and employment-screening decisions.[96] These services are particularly important to communities of color, where limited income, weak credit, and criminal-justice histories can combine as barriers to obtaining basic necessities.[97] Privacy provisions of the Fair Credit Reporting Act (FCRA)[98] (along with provisions of the Restore Online Shoppers Confidence Act[99] and the Telemarketing Sales Rule[100]) were deployed in a lawsuit brought by the FTC and Department of Justice. The suit alleged that MyLife.com violated the

---

87. *See* FED. TRADE COMM'N, *supra* note 9, at 7-9 (discussing automobiles); *id.* at 10-11 (discussing for-profit schools and education debt).

88. *Id.* at 12 (examining prepaid calling cards that could not be used to make calls).

89. *Id.* at 21-22 (exploring predatory payday loans).

90. *Id.* at 14-15 (considering magazines sold for delivery to prison that are never delivered).

91. *Id.* at 16-20.

92. *Id.* at 1.

93. *Id.* at ("Since 2016, the FTC has brought more than 25 actions where the agency could identify that the conduct either specifically targeted or disproportionately impacted communities of color.").

94. *Id.* at 6-22 (describing FTC enforcement actions).

95. *MyLife.com, Inc.*, FED. TRADE COMM'N (July 27, 2020), https://www.ftc.gov/enforcement/cases-proceedings/182-3022/mylifecom-inc [https://perma.cc/5PEW-GRQH].

96. *Protect & Improve Your Reputation Profile & Public Reputation Score. Check Out Anyone Else's*, MYLIFE.COM, https://www.mylife.com/showRegistration.pub [https://perma.cc/62YE-2SJ4].

97. *See* FED. TRADE COMM'N, *supra* note 9, at 4.

98. 15 U.S.C. § 1681 (2018).

99. *Id.*. §§ 8401-8405.

100. 16 C.F.R. § 310 (2021).

FCRA by "failing to maintain reasonable procedures to verify how its reports would be used, to ensure the information was accurate, and to make sure that the information it sold would be used by third parties only for legally permissible purposes."[101] The suit also importantly alleged that defendant MyLife.com fraudulently enticed consumers into purchasing automatically renewing subscriptions to its services by providing them with false and unverified information about their own backgrounds and others, including criminal histories, and that MyLife.com lacked procedures for both determining the accuracy of information and providing user notices.[102] Although the district court denied the defendant's motion to dismiss[103] and granted the government partial summary judgment, the court did not grant summary judgment on the FCRA privacy-related claims.[104] The suit resulted in an injunction and $21 million in civil penalties.[105]

More enforcement lawsuits of this type, that make use of existing law and the FTC's unfair-trade-practice authority, could help deter online predatory practices and shrink the Black Opticon. I believe that future litigation enforcing new race-conscious privacy laws enacted to address discriminatory predation and the disparate impact of data abuses on people of color could help even more.

* * *

To reiterate, Part I has illustrated the three sets of data-protection problems that comprise the Black Opticon. The Geofeedia incident, discussed in Section I.A, demonstrated panoptic problems of oversurveillance. Oversurveillance undermines African Americans' sense of security and fair play by placing their lives under a level of scrutiny other groups rarely face, exacerbating the problem of unwarranted encounters with the criminal-justice system. Facebook's discriminatory advertisements, discussed in Section I.B, embodied ban-optic problems of racially targeted exclusion from opportunity. Ban-optic

---

**101.** Press Release, Fed. Trade Comm'n, FTC Alleges California Purveyor of Background Reports Misled Consumers to Think Its Reports on Individuals Might Contain Criminal and Other Records (July 27, 2020), https://www.ftc.gov/news-events/press-releases/2020/07/ftc-alleges-california-purveyor-background-reports-misled [https://perma.cc/ZRE6-3ZKP].

**102.** Complaint for Permanent Injunction, Equitable Relief, Civil Penalties and Demand for Jury Trial at ¶¶ 9, 25-38, United States v. MyLife.com, Inc., 499 F. Supp. 3d 757, 767 (C.D. Cal. 2020) (No. 20-cv-6692).

**103.** *Mylife.com, Inc.*, 499 F. Supp. 3d 757 (denying the defendant's motion to dismiss).

**104.** United States v. MyLife.Com, Inc., 2021 U.S. Dist. LEXIS 201777, at *23 (C.D. Cal. Oct. 19, 2021) (granting partial summary judgement for the United States and holding that banners classifying millions of people "as a criminal or potential criminal for reasons MyLife will not disclose unless and until the consumer purchases a subscription . . . [are] marketing practices [that] are deceptive and material as a matter of law, and violate Section 5 of the FTC Act"); *id.* at *35 (not granting summary judgement on the FCRA claims because "there are genuine issues of material fact with respect to the Government's FCRA claim").

**105.** *See* Press Release, Fed. Trade Comm'n, FTC, DOJ Obtain Ban on Negative Option Marketing and $21 Million for Consumers Deceived by Background Report Provider MyLife (Dec. 16, 2021), https://www.ftc.gov/news-events/press-releases/2021/12/ftc-doj-obtain-ban-negative-option-marketing-21-million-consumers [https://perma.cc/3QSX-JJ22].

practices online encase African Americans in a racial caste system whereby roles and opportunities are fixed by perception of race rather than need, merit, or ability.[106] Finally, the MyLife.com litigation, discussed in Section I.C, illustrated the con-optic problems of targeted fraud and deception. African Americans deserve the attention of marketplace opportunity, but on the same, more favorable terms extended to other groups.

The Black Opticon pays the wrong kinds of attention to African Americans, using the resources of internet platforms and other digital technologies to gather, process, and share data about who we are, where we are, and to what we are vulnerable. In Part II, I consider how and whether changes in the design and enforcement of privacy law could help combat the Black Opticon.

## ii. an african american online equity agenda

This Part considers whether legal approaches premised on privacy law hold promise for African Americans seeking to escape the Black Opticon. To gauge that promise, I lay out an African American Online Equity Agenda (AAOEA) and use it to evaluate whether a new state law in Virginia, new privacy protection resources for the FTC, or a proposed new federal privacy agency embody assumptions and goals calculated to advance the interests of African Americans.

### *A. Escaping the Black Opticon: Paths Forward*

Calls for improved platform governance flow from many sources, including from platform company leaders themselves.[107] Advocates have called repeatedly for platform governance that includes privacy and data-protection law reform and industry self-governance to improve online data protections.[108] Platforms have sometimes responded to episodes of intense criticism from organized groups with changes in policy and practice.[109]

---

**106.** *Cf.* ISABEL WILKERSON, CASTE: THE ORIGINS OF OUR DISCONTENTS 18 (2020) (explaining that in the American caste system, race is a rank based on outwards traits that determines roles and opportunities).

**107.** *See, e.g.*, Samuel Stolton, *Zuckerberg Appeals for European Leadership on Platform Regulation*, EURACTIVE (May 19, 2020), https://www.euractiv.com/section/digital/news/zuckerberg-appeals-for-european-leadership-on-platform-regulation [https://perma.cc/8AUP-JZ6P]. *But see* Kevin Roose, *Facebook's "Supreme Court" Tells Zuckerberg He's the Decider*, N.Y. TIMES (May 6, 2021), https://www.nytimes.com/2021/05/06/technology/facebook-oversight-board-trump.html [https://perma.cc/UT7H-JNF5].

**108.** *See* Robert Gorwa, *What Is Platform Governance?*, 22 INFO. COMMC'N & SOC'Y 1, 1-2 (2019) (observing that regulatory proposals for curbing power of "digital giants" range from calls to break up Facebook to holding platforms legally responsible for content posted by users).

**109.** Consider, for example, Facebook's decision in November 2021 to end facial-recognition tagging, *see* Jerome Pesenti, *An Update on Our Use of Facial Recognition*, META (Nov. 2, 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition [https://perma.cc/5X3K-UTLG], after years of complaints by privacy advocates, including the Electronic Privacy Information Center, *see Facebook Abandons Facial Recognition System Long Targeted by EPIC*, ELEC. PRIV. INFO. CTR. (Nov. 2, 2021), https://epic.org/facebook-abandons-facial-recognition-system-long-targeted-by-epic [https://perma.cc/9ZYL-UMBZ].

Minority-group advocates have had some success directly pressuring industry, raising hopes for industry self-governance. For example, the advocacy group Color of Change aptly credits itself with persuading Facebook to conduct a civil-rights audit of its policies that respected white-nationalist content; persuading Google to ban predatory lending apps from Google Play to protect Black people from unreasonable terms, high default rates, and manipulation; and persuading Pinterest to stop featuring plantation wedding and party venues implicitly glorifying the heinous slave economy.[110] Successful interventions spurring voluntary change responsive to panoptic, ban-optic, and con-optic threats have occurred, but I speculate that they may be more the exception than the rule, especially since smaller platforms' abuses may fly under the radar of public-interest advocates. Voluntary self-governance to date has left African Americans vulnerable to lost privacy, data abuses, and social and economic inequity.[111]

Legislative reform is in the mix of proposed governance solutions as commentators vigorously debate the relative merits of law, data trusts,[112] content moderation, social-media councils, platform design, and norms.[113] Regimes of data-privacy law, antitrust law, intellectual-property law, constitutional law, civil-rights law, and human-rights law all bear on platform

---

**110.** *See Join Our Movement*, COLOR OF CHANGE, https://act.colorofchange.org/signup/signup [https://perma.cc/5FSL-SD9L] (listing organizational accomplishments). *See generally* Taylor Owen, *Introduction: Why Platform Governance?*, CTR. FOR INT'L GOVERNANCE INNOVATION (Oct. 28, 2019), https://www.cigionline.org/articles/introduction-why-platform-governance [https://perma.cc/ZD5Y-S827] ("[I]ssues that fall under this [platform governance] policy rubric are necessarily broad. . . . [D]ata privacy, competition policy, hate speech enforcement, digital literacy, media policy and governance of artificial intelligence (AI) all sit in this space.").

**111.** *Cf.* Erin Simpson & Adam Conner, *How to Regulate Tech: A Technology Framework for Online Services*, CTR. FOR AM. PROGRESS (Nov. 16, 2021), https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services [https://perma.cc/9TPF-DSF2 ] (reporting that people of color are susceptible to privacy harms stemming from online services, and Black and Hispanic people to privacy harms of oversurveillance and overpolicing).

**112.** The data trust is an old 1970s idea gaining renewed interest. *Cf.* MILLER, *supra* note 52, at 216-20 (arguing that information trusts are an imperfect solution and federal legislation is needed).

**113.** *See, e.g.*, Roger McNamee, *Big Tech Needs to Be Regulated. Here Are 4 Ways to Curb Disinformation and Protect Our Privacy*, TIME (July 29, 2020, 10:05 AM EDT), https://time.com/5872868/big-tech-regulated-here-is-4-ways [https://perma.cc/8K8Y-P44X] (arguing that big tech needs to be regulated to protect privacy); Mark MacCarthy, *To Regulate Digital Platforms, Focus on Specific Business Sectors*, BROOKINGS (Oct. 22, 2019), https://www.brookings.edu/blog/techtank/2019/10/22/to-regulate-digital-platforms-focus-on-specific-business-sectors [https://perma.cc/7ZDH-VQRS] (arguing for sector-specific regulation); D. Daniel Sokol & Marshall Van Alstyne, *The Rising Risk of Platform Regulation*, MIT SLOAN MGMT. REV. (Nov. 11, 2020), https://sloanreview.mit.edu/article/the-rising-risk-of-platform-regulation [https://perma.cc/R636-YLN7] (arguing for proactive self-regulation by technology platforms to avoid eroding "the powerful network effects that drive their growth and benefit their users").

governance.[114] Due to the major inadequacies of existing measures, I urge new privacy and data-protection legal measures as requirements of adequate platform governance.[115] Federal privacy-law reform is urgently needed to protect the interests of all Americans, including African Americans. Recently proposed federal legislation[116] and a proposed expansion of the FTC's privacy and data-protection capacities are generally commendable,[117] as is recently enacted state privacy legislation in California, Colorado, and Virginia.[118] However, they must be assessed through the lens of race to determine whether they address the oversurveillance, exclusion, and scamming characteristic of the Black Opticon.

### *B. Generic Versus Explicitly Group-Specific Reform Guidance*

To adequately confront the Black Opticon, data-privacy reforms should explicitly address group-specific harms, not just general harms. Existing guidance around data-privacy reform falls short of directly addressing the pervasive problems of African Americans in the digital economy—even when it purports to promote equity. Consider, for example, the Civil Rights Privacy and Technology Table (CRPTT), a consortium of leading civil-rights organizations and

---

**114.** *See, e.g.*, Winifred R. Poster, *Racialized Surveillance in the Digital Service Economy*, *in* CAPTIVATING TECHNOLOGY: RACE, CARCERAL TECHNOSCIENCE, AND LIBERATORY IMAGINATION IN EVERYDAY LIFE 133 (Ruha Benjamin ed., 2019); Tamara K. Nopper, *Digital Character in "The Scored Society": FICO, Social Networks, and Competing Measurements of Creditworthiness*, *in* CAPTIVATING TECHNOLOGY, *supra*, at 170; Mitali Thakor, *Deception by Design: Digital Skin, Racial Matter, and the New Policing of Child Sexual Exploitation*, *in* CAPTIVATING TECHNOLOGY, *supra*, at 188; Madison Van Oort, *Employing the Carceral Imaginary: An Ethnography of Worker Surveillance in the Retail Industry*, *in* CAPTIVATING TECHNOLOGY, *supra*, at 209; VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 11 (2018) (proposing and discussing various approaches to platform regulation).

**115.** Anita L. Allen, *A New Digital Age Privacy Protection Agency Holds Promise*, REGUL. REV. (Aug. 9, 2021), https://www.theregreview.org/2021/08/09/allen-new-digital-age-privacy-protection-agency-holds-promise [https://perma.cc/K3BB-E9RM].

**116.** *See* Press Release, Kirsten Gillibrand, U.S. Sen., Gillibrand Introduces New and Improved Consumer Watchdog Agency to Give Americans Control over Their Data (June 17, 2021), https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-new-and-improved-consumer-watchdog-agency-to-give-americans-control-over-their-data [https://perma.cc/WA7Z-WDEZ] (proposing legislation creating a new Data Protection Agency because technology firms are not adequately self-regulating and the Federal Trade Commission has failed to adequately respond).

**117.** *See* H. COMM. ON ENERGY & COM., *supra* note 26; *see also U.S. House Committee Votes to Create New FTC Privacy Bureau and Appropriate $1 Billion to the Agency*, NAT'L L. REV. (Sept. 16, 2021), https://www.natlawreview.com/article/us-house-committee-votes-to-create-new-ftc-privacy-bureau-and-appropriate-1-billion [https://perma.cc/V4K3-QYS4] (reporting that the U.S. House Committee on Energy and Commerce approved a $1 billion budget for the FTC over 10 years "to create and operate a bureau to accomplish the Commission's work related to unfair or deceptive acts or practices relating to privacy, data security, identity theft, data abuses and similar matters"); *FTC Report to Congress on Privacy and Security*, FED. TRADE COMM'N 3 (Sept. 13, 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf [https://perma.cc/W2A4-QNR4] (describing the FTC's plan to "target its limited resources toward the most egregious and substantial privacy and security abuses")).

**118.** Legislation has been enacted in Virginia (assessed in Section II.C, *infra*), California, and Colorado. *See* Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to -585 (2021); California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-.199.100 (West 2021); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301 to -1313 (2021).

privacy advocates examining privacy through the lenses of marginalized communities. The CRPTT concluded that Congress should prioritize equity, ensuring "that technology serves all people in the United States, rather than facilitating discrimination or reinforcing existing inequities."[119] The CRPTT also announced a set of equity principles beneficial to all that it collectively believes should guide Congress in the prioritization of equity: "Ending High-Tech Profiling," "Ensuring Justice in Automated Decisions," "Preserving Constitutional Principles," "Ensuring that Technology Serves People Historically Subject to Discrimination," "Defining Responsible Use of Personal Information and Enhancing Individual Rights," and "Making Systems Transparent and Accountable."[120]

Some of the CRPTT's principles are facially generic for improving privacy and data protection for all people—namely, for promoting responsible information use, maintaining the Constitution, enhancing rights, and promoting transparent and accountable systems.[121] One principle invokes communities of color: "ensuring that technology serves people historically subject to discrimination" in access to goods and services.[122] Two other principles do not invoke African Americans explicitly, but are critical to dismantling the Black Opticon. These principles are "ending high-tech profiling" and "ensuring justice in automated decisions."[123] As I discussed in Part I, concerns about negative profiling and algorithmic injustice are high on the list of African American concerns about platform inequities. The CRPTT principles support abating wrongfully discriminatory oversurveillance, exclusion, and predation.

At this critical time of exploding technology and racial conflict, I believe that policy making should be explicitly antiracist. In addition to considering agendas concerning the general population, which are appropriate and foster strategic coalition building, policy makers should welcome and rely upon group-specific agendas for guidance and articulate race-based rationales for reform measures intended to protect data and data privacy. This dual approach, which can be termed "policy making for all and policy making for some," will help to ensure that the interests of marginalized racial minorities are not overlooked, and aid in surfacing possible conflicts between the interests of one racialized group and other groups. For example, targeting Black men for high-tech modes of data surveillance based on race may address concerns of a majority about freedom from crime, but violate Black men's entitlement to privacy and freedom from racist social control. The agenda I offer for assessing whether recent and

---

**119.** *Civil Rights, Privacy, and Technology: Recommended 2021 Oversight Priorities for the 117th Congress*, C.R. PRIV. & TECH. TABLE 2 (Jan. 27, 2021), https://www.civilrightstable.org/wp-content/uploads/2021/01/Civil-Rights-Privacy-and-Technology-Recommended-2021-Oversight-Priorities.pdf [https://perma.cc/AEE7-MELL].

**120.** *See Principles*, C.R. PRIV. & TECH. TABLE, https://www.civilrightstable.org/principles [https://perma.cc/45ZA-R6NV].

**121.** *Id.*

**122.** *Id.*

**123.** *Id.*

pending legal reforms will help African Americans escape the Black Opticon is in precisely the same spirit as those adopted by the CRPTT, but toward the specific goal of disabling the Black Opticon. I specifically reference the African American experience through an African American Online Equity Agenda.

The keystone of the AAOEA is to direct design of privacy and data-protection-law policy reforms directly to pervasive problems of African Americans in the digital economy. Characterizing a Black Opticon of disparity and disadvantage is my way of succinctly denoting pervasive problems African Americans are facing online. While the Black Opticon frames my response to recent legal enactments and proposals, the AAOEA centers on five points of guidance for race-conscious, antiracist law and policy making, articulated as goals[124]:

1. **Racial inequality nonexacerbation goal:** Design privacy and data-protection policies recognizing that baseline data privacy and the power data privacy confers may be unequally distributed along racial lines in society, and that racial inequalities should not be exacerbated.
2. **Racial impact neutrality goal**: Design privacy and data-protection policies acknowledging that ostensibly race-neutral privacy policies may not have race-neutral effects or protect all groups equally.
3. **Race-based discriminatory oversurveillance elimination goal**: Design privacy and data-protection policies that disable automated and nonautomated invasive and excessive surveillance, monitoring, profiling, tracking, and identification of African Americans.
4. **Race-based discriminatory exclusion reduction goal**: Design privacy and data-protection policies aimed at prohibiting online advertising and marketing practices that exclude and wrongly discriminate on the basis of African American race or characteristics that are its proxies, including phenotypes, names, places of residence, or associations.
5. **Race-based discriminatory fraud, deceit, and exploitation reduction goal**: Design privacy and data-protection policies aimed at reducing fraud, deceit, and scams targeting African American consumers and exploiting their socioeconomic vulnerabilities.

In the next Section, I reference these agenda items to assess features of the recently enacted Virginia Consumer Data Protection Act, the proposed creation of an FTC privacy bureau, and a bill proposing an independent federal privacy agency. Although none of these potential reforms are dedicated to Big-Tech platform governance, comprehensive privacy and data-protection reforms generally bear on regulation of the digital economy with implications for the equitable regulation of personal-data processing by all online platforms.

---

124. Other racialized minority groups could adopt these principles to advance their groups' interests, but these principles were formulated with the experiences of African Americans in mind, and I do not contend that all five points of guidance are equally relevant to all racial groups.

### C. *Assessing Enacted State Law: Virginia Consumer Data Protection Act (2021)*

American privacy law has become a fast-evolving field. State legislation already on the books in 2022 will surely be followed by additional state and federal measures, all of which are likely to reflect the global influence of the European Union's 2018 General Data Protection Regulation (GDPR).[125] At least six states—New York, Pennsylvania, Minnesota, North Carolina, and Ohio—were actively considering privacy and data-protection legislation in early 2022.[126] The anticipated explosion of nonidentical state law may prompt a comprehensive federal measure, if only to rescue the national business sector from the inefficiencies of compliance with dozens of potentially inconsistent state regimes. In 2018, California became the first U.S. state to adopt a comprehensive data-protection law, and its reforms are still unfolding after a statewide ballot initiative expanded and amended the law in November 2020.[127] Virginia came next with a comprehensive statute in March 2021,[128] followed by Colorado.[129] Although the Virginia statute borrowed from the GDPR and California measures, it differs significantly from both.

Looking at privacy and data-protection law through a lens of the Black Opticon, the Commonwealth of Virginia Consumer Data Protection Act (2021) (VCDPA) holds special interest as a case study in possibility and disappointment. Of the first three states (including California and Colorado) to exact comprehensive new privacy and data-protection statutes, Virginia is the only state that belonged to the former Confederacy.[130] It is now saddled with a highly visible legacy of African American slavery and legally enforced racial segregation.[131] Virginia has a larger share of African American residents than

---

**125.** Commission Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.

**126.** Sarah Rippy, *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PROS. (Sept. 16, 2021), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/W89S-HL4F] (noting that all but fifteen states had recently had consumer data-privacy legislation in some stage of consideration as of November 1, 2021).

**127.** California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-199.100 (West 2021).

**128.** Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to -585 (2021).

**129.** Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301 to -1313 (2021).

**130.** The "Confederacy" refers to the states that broke away from the United States, beginning in 1861, precipitating the Civil War. The confederate states included Texas, Arkansas, Louisiana, Tennessee, Mississippi, Alabama, Georgia, Florida, South Carolina, North Carolina and Virginia. *See* Joanne Freeman, *Timeline of the Civil War: 1861*, LIBR. CONG., https://www.loc.gov/collections/civil-war-glass-negatives/articles-and-essays/time-line-of-the-civil-war/1861 [https://perma.cc/S72Y-LTKB]; *Civil War Facts: 1861-1865*, NAT'L PARK SERV. (Oct. 27, 2021), https://www.nps.gov/civilwar/facts.htm [https://perma.cc/8ES9-5FBY].

**131.** *See* Michael E. Ruane, *Virginia Is the Birthplace of Slavery and Segregation-and It Still Can't Escape That Legacy*, WASH. POST (Feb. 6, 2019), https://www.washingtonpost.com/history/2019/02/06/virginia-is-birthplace-american-slavery-segregation-it-still-cant-escape-that-legacy [https://perma.cc/B8RY-S62E]; Brendan Wolfe, *Racial Integrity Laws (1924-1930)*, ENCYCLOPEDIA VA. (Feb. 25, 2021), https://encyclopediavirginia.org/entries/racial-integrity-

either of the other early adopter states. Indeed, approximately twenty-one percent of Virginians are African American, compared to seven percent of Californians and just five percent of Coloradoans.[132] An ethnically and racially diverse group of legislators sponsored the VCDPA, including its "chief patron," African American Assemblyman Cliff Hayes.[133]

The VCDPA, which will go into full effect January 1, 2023, boasts general antidiscrimination provisions,[134] but it does not explicitly reference the interests of African Americans or antiracism as a legislative goal. No strong evidence, such as records of legislative debate, preambles, findings, or express provisions, displays conscious recognition of the first two AAOEA agenda items: that baseline privacy and its associated powers may be unequally distributed along racial lines in society, and that race-neutral laws may not have race-neutral effects.

Neither a civil-rights law nor an online-platform-governance measure as such, the VCDPA enacts a race-neutral consumer-information-protection regime applicable to businesses on behalf of all Virginians.[135] The statute does not target global platform companies, but would apply to online companies of a certain size doing business in the state or with its resident consumers. Big Tech

---

laws-1924-1930 [https://perma.cc/H5FX-D5DP]. Of course, Virginia is not the only state with a legacy of legally enforced racial segregation. *See, e.g.*, JEAN PFAELZER, DRIVEN OUT: THE FORGOTTEN WAR AGAINST CHINESE AMERICANS (2007) (exploring discrimination and exclusion of Chinese immigrants and citizens in California).

132. *Black Population by State 2021*, WORLD POPULATION REV., https://worldpopulationreview.com/state-rankings/black-population-by-state [https://perma.cc/U8JW-LEXQ].

133. For a list of VCDPA "patrons," see *2021 Special Session 1*, VA.'S LEGIS. INFO. SYS, https://lis.virginia.gov/cgi-bin/legp604.exe?212+mbr+HB2307 [https://perma.cc/3NKW-LWD9]. For information on their backgrounds, see *Welcome*, CLIFF HAYES, https://cliffhayes.com [https://perma.cc/Y8NU-YXEB]; *Meet Hala*, HALA FOR VA., https://www.halaforvirginia.com [https://perma.cc/VGU5-TT3X]; *Home*, LAMONT BAGBY, https://www.lamontbagby.org [https://perma.cc/FYN9-GVMV]; *About Suhas*, SUHAS SUBRAMANYAM, https://www.suhasforvirginia.com/about-suhas [https://perma.cc/F7DD-PYQC]; *Meet Delegate Mark Levine*, MARK FOR DELEGATE, https://www.markfordelegate.com/bio [https://perma.cc/3P46-ZZT9]; *Meet Martha*, MUGLER FOR DELEGATE, https://www.muglerfordelegate.com/meet-martha [https://perma.cc/9PQZ-QLNS]; and *About Dave*, DAVE MARSDEN FOR SENATE, https://marsdenforsenate.nationbuilder.com [https://perma.cc/FLX6-HKY9].

134. *See* VA. CODE ANN. § 59.1-578(A)(4) (2021) ("A controller shall . . . [n]ot process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer."). Under the Virginia statute, consumers can opt out of discrimination protections. *See id.* ("However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-577 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.").

135. *See id.* § 59.1-575-§ 59.1-585. The statute is "race-neutral" in the sense that neither its definition of "sensitive data" at § 59.1-575, nor its nondiscrimination provisions, *e.g.*, § 59.1-578(A) (3), mention a specific racial group.

firms, including Microsoft and Amazon, fully endorsed the statute.[136] Future of Privacy Forum, an organization supported by platforms such as Facebook, Google, and Twitter, praised it as a "significant milestone."[137] But critics have described the Virginia law as weak—even "empty."[138]

Under the statute, consumers have a right to access, correct, remove and know about "personal data" processed by data "controllers."[139] Data "controller" is a term borrowed from the GDPR, defined in the VCDPA as an entity that determines the means or purposes of data "processing," which includes, among other things, the "collection, use, storage, disclosure, analysis, deletion, or modification of personal data."[140] Data controllers are responsible for data minimization, meaning that they may not process more personal data than needed nor process personal data for purposes other than those for which it was originally authorized and processed absent explicit consumer consent.[141] The VCDPA defines "personal data" to include "any information that is linked or reasonably linkable to an identified or identifiable natural person," but excludes employment data, as well as "pseudonymous," "de-identified," and "publicly available" information.[142] Like Article 28 of the GDPR, the VCDPA requires that data controllers execute processing agreements with partnering data processers.[143] A key feature adapted from the GDPR, the VCDPA requires "data protection assessments" of consumer risks and benefits.[144] While the details are unclear, such assessments could be required as a precondition even of consensual algorithmically aided targeted advertising, the use of AI and profiling, where there is a "reasonably foreseeable risk" that they could lead to a discriminatory impact, privacy invasion, or other harm.[145]

---

**136.** *See* Graham Moomaw, *Virginia's New Big Tech-Backed Data Privacy Law Is the Nation's Second. Critics Say It Doesn't Go Far Enough*, VA. MERCURY (Mar. 30, 2021, 12:03 AM), https://www.virginiamercury.com/2021/03/30/virginias-new-big-tech-backed-data-privacy-law-is-the-nations-second-critics-say-it-doesnt-go-far-enough [https://perma.cc/PT7Q-QRP5] ("The Future of Privacy Forum, a data privacy think tank supported by corporate benefactors such as Google, Amazon, Facebook and Twitter as well as the Bill and Melinda Gates Foundation and the Robert Wood Johnson Foundation, hailed the passage of the Virginia bill as a 'significant milestone' on a national issue.").

**137.** *Id.*

**138.** *See* Hayley Tsukayama, *Virginians Deserve Better than This Empty Privacy Law*, ELEC. FRONTIER FOUND. (Feb. 12, 2021), https://www.eff.org/deeplinks/2021/02/virginians-deserve-better-empty-privacy-law [https://perma.cc/6FVP-SAVY].

**139.** VA. CODE ANN. § 59.1-577 (2021) (addressing personal data rights of consumers).

**140.** *Id.* § 59.1-575 ("Definitions.").

**141.** *Id.* § 59.1-578(A)(1)-(2).

**142.** *Id.* §§ 59.1-575, 59.1-581(B), (D) ("Processing de-identified data; exemptions.").

**143.** *Id.* § 59.1-579 ("Responsibility according to role; controller and processor.").

**144.** *Id.* § 59.1-580 ("Data protection assessments.").

**145.** Jeremy Feigelson, Avi Gesser, Robert Maddox, Christopher Garrett, Anna Gressel, Alexandra P. Swain, Javier Alvarez-Oviedo, Tricia Reville & Scott M. Caravello, *Virginia Enacts a Comprehensive Privacy Law – Similarities and Differences Among VCDPA, CCPA and GDPR*, DEBEVOISE & PLIMPTON (Mar. 4, 2021),

On behalf of all Virginia consumers, the VCDPA governs the many activities of larger private-sector, nongovernmental data controllers, exempting from reach massive sectors of the economy, including state government and its subdivisions; HIPAA "covered entities"; financial institutions or data subject to the Gramm-Leach-Bliley Act; data subject to the federal Fair Credit Reporting Act; and data related to vehicle driver information, subject to the federal Driver's Privacy Protection Act of 1994.[146] Moreover the statute's requirements do not apply to nonprofits, higher-education institutions, or employment activities.[147]

When these VCDPA coverage exemptions are assessed through the lens of the AAOEA, it becomes clear that they may lessen the VCDPA's capacity to eliminate forms of oversurveillance, exclusion and predation online likely experienced by African Americans in Virginia. As a group, Black Virginians have fewer educational and financial resources than some other racial groups in the state; about sixteen percent of the state's African American residents, as compared to just eight percent of the state's white residents, live in poverty and are vulnerable to financial exploitation and abuses.[148] Slightly over fourteen percent of Virginia's adult Black female residents and seventeen percentage of the state's Black male residents lack a high school degree.[149] Only twenty-five percent of Black women and twenty percent of Black men hold a college degree, the lowest college-graduation percentage of any Virginia racial or ethnic group reported.[150] Discriminatory credit, employment, educational, and financial decisions are likely common experiences of African Americans in Virginia, as they are elsewhere in the nation, and persist in the face of existing federal privacy and civil-rights laws.[151]

---

https://www.debevoisedatablog.com/2021/03/04/virginia-enacts-a-comprehensive-privacy-law-similarities-and-differences-among-vcdpa-ccpa-and-gdpr [https://perma.cc/ARA8-WQH2] (quoting VA. CODE ANN. § 59.1-580(A)(3) (2021)).

**146.** VA. CODE ANN. § 59.1-576(A)-(D) (2021); *see also id.* § 59.1-582 (establishing limitations on coverage).

**147.** *Id.* § 59.1-576(B), (C)(14).

**148.** *Poverty Rate by Race/Ethnicity*, KFF (2019), https://www.kff.org/other/state-indicator/poverty-rate-by-raceethnicity/?currentTimeframe=0&selectedRows=%7B%22states%22:%7B%22virginia%22:%7B%7D%7D%7D&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D [https://perma.cc/D37T-PGNJ].

**149.** *See Education Attainment in Virginia*, STAT. ATLAS, https://statisticalatlas.com/state/Virginia/Educational-Attainment. For somewhat different numbers, see *Educational Attainment in Virginia*, FED. RSRV. BANK RICHMOND (2019), https://www.richmondfed.org/-/media/richmondfedorg/research/regional_economy/reports/special_reports/pdf/educational_attainment_va.pdf [https://perma.cc/UG3N-P8NU].

**150.** *See* FED. RSRV. BANK RICHMOND, *supra* note 149.

**151.** *Cf.* VA. AFR. AM. HIST. EDUC. COMM'N, FINAL REPORT OF THE VIRGINIA COMMISSION ON AFRICAN AMERICAN HISTORY EDUCATION IN THE COMMONWEALTH 7 (Aug. 2020), https://www.governor.virginia.gov/media/governorvirginiagov/secretary-of-education/pdf/AAHEC-Report-Final_version2.pdf [https://perma.cc/J9ZD-Y5ZQ] ("Black people in Virginia endured not only decades of enslavement, but also Jim Crow terror and discrimination, Massive Resistance, and modern day iterations and remnants of government sanctioned Black oppression. Virginia has failed to fully represent African Americans in its history, contributing to a legacy of racism that has seeped into systems that impact every individual and every aspect of American life, including our classrooms."). One notes that the official website of

The shape that the VCDPA took as a consumer-protection law targeting larger businesses not regulated by federal privacy laws may reflect practical strategies and compromises needed for speedy passage of any politically acceptable bill.[152] Specifically, speedy passage may have been enabled by exclusions calculated to skirt federal preemption concerns under the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley, the Fair Credit Reporting Act, the Drivers Protection Act, and the Children's Online Privacy Protection Act (COPPA), decades-old laws that themselves have not adequately protected African Americans.

But avoiding federal preemption would not explain all of the VCDPA's sector exclusions. The rationale for exempting all nonprofits regardless of size—as well as commonwealth governmental entities, including the police, jails, and prisons[153]—is unclear, but likely relate to a felt need to make the legislation,

---

Fairfax County, Virginia is replete with antidiscrimination resources. *See Human Rights and Equity Programs*, FAIRFAX CNTY., https://www.fairfaxcounty.gov/humanrights/brochures-and-publications [https://perma.cc/XSU2-QEM6] (providing information helping Fairfax residents and visitors understand their rights with regard to employment, education, housing, public accommodations, and credit). Fairfax County's Black population is 10.6%, *see QuickFacts: Fairfax County, Virginia*, U.S. CENSUS BUREAU (July 1, 2021), https://www.census.gov/quickfacts/fact/table/fairfaxcountyvirginia/PST045221 [https://perma.cc/6PVN-RMMZ], whereas Richmond Country, Virginia, whose population is 29.6% Black, *see QuickFacts: Richmond County, Virginia*, U.S. CENSUS BUREAU (July 1, 2021), https://www.census.gov/quickfacts/fact/table/richmondcountyvirginia/PST045221 [https://perma.cc/4R8A-GEAN], lacks similar antidiscrimination resources on its website, *see Welcome to Richmond County*, RICHMOND CNTY., https://co.richmond.va.us/about-us [https://perma.cc/W3A5-DJZF].

152. *See Virginia Passes Comprehensive Privacy Law*, GIBSON DUNN (Mar. 8, 2021), https://www.gibsondunn.com/virginia-passes-comprehensive-privacy-law [https://perma.cc/9SHD-R9XW] ("Without the time to lengthily debate controversial issues that caused similar proposals in other states to die – such as the scope of a private right of action – the VCDPA focuses on privacy rights and obligations, over which there has been general consensus."). State legislators introduced the Virginia Consumer Data Protection Act (VCDPA) in a very brief legislative session in early 2021. During this session, legislators focused on areas in which consensus could be achieved, such as consumer-rights and business-sector obligations, but did not have time for lengthy debate. *See 2021 Session: SB 1392 Consumer Data Protection Act*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392 [https://perma.cc/DG2F-22T3]. On February 8, 2021, the House reconciliation process was complete. *See 2021 Special Session I: HB 2307 Consumer Data Protection Act*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+HB2307 [https://perma.cc/2DRJ-24JD]. The VCDPA was signed by Governor Ralph Northam less than a month later, on March 2, 2021. *See* Cat Zakrzewski, *Virginia Governor Signs Nation's Second State Consumer Privacy Bill*, WASH. POST (Mar. 2, 2021, 8:17 PM EST), https://www.washingtonpost.com/technology/2021/03/02/privacy-tech-data-virgina [https://perma.cc/2WJX-AP8M]; *cf.* Joseph Duball, *Virginia Data Protection Act on the Horizon—Now What?*, IAPP (Feb. 4, 2021), https://iapp.org/news/a/virginia-consumer-data-protection-act-on-the-horizon-now-what [https://perma.cc/85AF-KEF4] (observing minimal opposition to the bill outside of discussion on the private right of action, and opining that Virginia's approach "offers some lessons about how to get things done").

153. VA. CODE ANN. § 59.1-576(B) (2021) ("This chapter shall not apply to any (i) body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial institution or data subject to Title V of the

which passed unanimously and quickly, uncontentious.[154] The exemptions represent a lost opportunity to regulate or ban the use of facial-recognition technology by airports and state police,[155] or to regulate business practices that involve public-private partnerships that scaffold the Black Opticon, as seen in the Geofeedia example.[156] Because the VCDPA does not apply across the board to government entities, it does not address the threat of law-enforcement or public-agency oversurveillance, monitoring, tracking, profiling, or identification. Photographs and data based on photographs commonly used for facial-recognition analytics are excluded from "biometric" data protected under the statute,[157] and these could presumably be shared by private platforms with Virginia authorities. While use of photographic data has a place in law enforcement, machine and human errors in the use of such data disproportionately impact African Americans.[158]

The VCDPA explicitly forbids the processing of personal data in violation of state and federal antidiscrimination laws.[159] This is a plus from the point of view advanced by the AAOEA and the call for race-conscious privacy law, since many of the nation's antidiscrimination laws refer to "race" discrimination and were enacted specifically to address the wounds and scars of slavery and Jim Crow. A "controller," defined as "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data,"[160] is not permitted to provide different goods, services, or prices on a discriminatory basis.[161] However, toxic forms of discrimination can creep in. The statute does not disallow targeted advertising—a practice known to be used discriminatorily to exclude Black people from opportunities and to facilitate predation[162]—but

---

federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); (iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit organization; or (v) institution of higher education.").

154. *See supra* note 151 and accompanying text.

155. Legislation passed in Virginia in 2021 banned facial-recognition technology being bought or used by local police, sheriffs, and campus police without the approval of the state legislature. *See* 2021 Va. Acts ch. 537. The original bill was introduced by Delegate Lashrecse D. Aird, an African American woman, *2021 Special Session I*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+HB2031 [https://perma.cc/B4TQ-RWSV].

156. *See supra* notes 57-64 and accompanying text.

157. VA. CODE ANN. § 59.1-575 (2021).

158. *See, e.g.*, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/WXH6-UJH3] (telling the story of Nijeer Parks, a thirty-three-year-old Black man who sued the New Jersey police after being arrested and jailed for ten days for a crime he did not commit).

159. VA. CODE ANN. § 59.1-578(A)(4) (2021).

160. *Id.* § 59.1-575 (defining "controller").

161. *Id.* § 59.1-578(A)(4).

162. *Cf.* Jinyan Zang, *Solving the Problem of Racially Discriminatory Advertising on Facebook*, BROOKINGS (Oct. 19, 2021), https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook [https://perma.cc/S8KQ-BSCX] ("[R]egulators, advocacy groups, and industry must directly address these issues with Facebook and other advertising platforms to ensure that online advertising is transparent and fair to all Americans.").

gives consumers the right to opt out of targeted advertising.[163] Consumers can opt out of data processing used for profiling, but only if they have knowledge that such processing is or could be taking place. Consumer opt-out rights will only be meaningful if businesses facilitate the process of opting out to thereby increase the chances that African American and other consumers understand how they can and why they might want to do so.[164]

The statute's privacy-notice requirement may help make opt-out rights somewhat more effective if the notices inform consumers of data uses consumers might wish to opt out of and the means and reasons for doing so.[165] And it may be relevant that the statute defines "consent" as "a clear affirmative act,"[166] arguably limiting businesses' ability to rely on opt-out consent. That said, according to an Electronic Frontier Foundation analysis, the statute allows firms to charge higher prices to consumers who opt out of targeted ads, sale of their data, and profiling.[167] This feature of the law raises a fundamental concern about discrimination reflected in the AAOEA's background assumption that privacy, a vital good, is unequally distributed in society. If data privacy has a price, low-income consumers may be unable to afford it and will thus become the law's privacy losers.[168] The business sector's interest in ad revenue must be assessed in the light of low-income consumers of color's weighty interests in not having to sacrifice important forms of data privacy to access platform services.

Like the GDPR, the VCDPA treats racial data as a category of "sensitive data," restricting the processing of data regarding racial or ethnic origin, religious

---

**163.** VA. CODE ANN. § 59.1-577(A)(5) (2021).

**164.** Critics of the VCDPA point to the opt-out provisions as a weakness of the law. *See, e.g.*, Irene Leech & Susan Grant, *We Need Real Privacy Protection in Virginia*, VA. MERCURY (Feb. 16, 2021, 12:34 AM), https://www.virginiamercury.com/2021/02/16/we-need-real-privacy-protection-in-virginia [https://perma.cc/N7SS-53DA] ("[The] Act places the burden on consumers to navigate today's incredibly complex data ecosystem. Under this weak bill, consumers must take steps to opt out of unwanted uses of their information (to the limited extent they are allowed to do so). Making 'opt out' the default disempowers consumers and poses equity concerns; consumers with less time and resources to figure out how their data is being used and how to opt out will inevitably be subject to more privacy violations. Where the default lies matters, as marketers well know. It's time to change the default to 'opt in.'").

**165.** VA. CODE ANN. § 59.1-578(E) (2021) ("A controller shall establish, and shall describe in a privacy notice . . . means for consumers to submit a request to exercise their consumer rights.").

**166.** *Id.* § 59.1-575.

**167.** Tsukayama, *supra* note 138 ("Virginia's privacy law also explicitly allows companies to engage in 'pay for privacy' schemes, which punish consumers for exercising their privacy rights. In Virginia's case, the bill says that consumers who opt-out of having their data used for targeted advertising, having it sold, or for profiling, can be charged a different 'price, rate, level, quality or selection of goods and services.' That means punishing people for protecting their privacy—a structure that ends up harming those who can't afford to protect themselves against data protection. Privacy should have no price tag.").

**168.** *Cf.* Lior J. Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2010 (2013) (arguing that privacy laws "create winners and losers").

beliefs, citizenship, and immigration status.[169] Article 9 of the GDPR provides that "[p]rocessing of personal data revealing racial or ethnic origin . . . shall be prohibited."[170] The GDPR regulates the collection of race and ethnicity data, although public interest and consent exceptions are allowed.[171] The VCDPA likewise allows some processing of race and ethnicity data.[172] It allows such processing with a consumer's consent,[173] suggesting that whether race data and its proxies ought to be available should be left to the individual to decide. Consent for race and ethnicity data processing must be an affirmative act, but it is unclear what will be deemed to constitute an affirmative act of opting into race data collection by those interpreting the law for enforcement purposes once it goes into effect in 2023.

Treating race as private and sensitive personal data under state law may be detrimental to the interests of marginalized people of color. In 2003, a so-called "Racial Privacy Initiative" to prohibit public entities from gathering and using race information was put to direct citizen referendum vote across California.[174] Widely opposed by communities of color fearing a disparate impact, an anti-affirmative-action agenda was indeed at the root of the Proposition 54 referendum.[175] Hopefully, the politics of race in Virginia will not inspire attempts to attack beneficial forms of affirmative action in education and employment based on the spirit or provisions of the VCDPA protecting race and ethnicity data from nonconsensual processing. Since employment and higher education are exempted from the statute, this worry may not be much warranted.[176] But without such exemptions, the neutral-seeming provision of the VCDPA limiting nonconsensual race and ethnicity data processing could have a disparate and negative impact on the interests of marginalized groups in private-sector race-conscious remedies and programs. Here, I invoke the "racial impact neutrality goal" of the AAOEA to assess legal reform. This goal requires privacy and data-protection policies to address whether neutral-appearing privacy policies assumed to protect all groups equally may have disparate impacts on African Americans.

---

**169.** VA. CODE ANN. § 59.1-575 (2021) ("'Sensitive data'" means a category of personal data that includes: 1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; 3. The personal data collected from a known child; or 4. Precise geolocation data.").

**170.** Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 9, § 1, 2016 O.J. (L 119) 1, 38 ("Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.").

**171.** *Id.* art. 9, § 2.

**172.** *See* VA. CODE ANN. § 59.1-576(C)(4) (2021).

**173.** *Id.* § 59.1-578(A)(5).

**174.** ALLEN, *supra* note 42, at 130-32 (recounting the Racial Privacy Initiative referendum effort in California).

**175.** *Id*. at 131 ("[N]ationally prominent opponents of affirmative action and so-called reverse discrimination supported the measure . . . .").

**176.** VA. CODE ANN. § 59.1-576(B), (C)(14) (2021).

Another neutral-seeming feature of the VCDPA may also have disparate impacts. The Virginia statute does not include a private right of action. Enforcement rests in the hands of the state Attorney General.[177] The Virginia Trial Lawyers Association opposed the VCDPA on the ground that it will subject its residents to the shifting winds of politics.[178] Were the duties of the Attorney General's office to fall into biased hands, state protection pursuant to the VCDPA might be allocated to Virginians on a racially discriminatory basis. The neutral-seeming feature of not providing for a private right of action could disparately impact African Americans, dependent upon the discretion of authorities to vindicate their rights, and especially in a state recovering from a long history of enslavement, forced racial segregation, and social prejudice. Here, I again invoke the "racial impact neutrality goal" of the AAOEA to suggest a basis for disappointment in legal reform.

Despite promising features that could help fight discriminatory data practices in the future, the VCDPA favors Virginia businesses over consumers, and leaves alone Big Tech platforms processing Virginians' personal data. While a complete assessment is premature, it is unlikely that the VCDPA on its own will do much to help dismantle the Black Opticon. Fortunately, some Virginia policy makers grasp the limitations of the statute relevant to the elimination of discriminatory oversurveillance, exclusion, and fraud. Of note, U.S. Senator Mark Warner described the VCDPA as merely a "first step."[179] Pertinent to the exclusionary surveillance-defeating goal of the AAOEA, Warner sees "the need to rein in so-called dark patterns, manipulative online tactics used to obtain more customer data."[180]

African American VCDPA sponsor Cliff Hayes has been careful not to overstate the law's significance as an answer to Virginians' privacy problems. Furthermore, he understands that the statute is not a major boon for Black Virginians. On the contrary, he publicly stated that the VCDPA was a step-wise

---

**177.** *Id.* § 59.1-584 (enforcement, civil penalties, and expenses).

**178.** *See* Hyung Jun Lee, *Virginia Lawmakers Advance Consumer Data Protection Act*, SUSSEX-SURRY DISPATCH (Feb. 25, 2021), https://www.thesussexsurrydispatch.com/news/virginia-lawmakers-advance-consumer-data-protection-act/article_59ee0df8-778e-11eb-b79c-b706a5fb2fb0.html [https://perma.cc/34XQ-96GX] ("Attorney Mark Dix spoke in opposition of the bill on behalf of the Virginia Trial Lawyers Association. He said the measure would hurt Virginians because it is 'going to close the courthouse doors.' 'It provides no cause of action whatsoever for the consumer, the person who is actually hurt,' Dix said. 'It provides no remedy whatsoever for the consumer.' Dix argued that having the attorney general's office handle the enforcement of this legislation limits the consumer. Using a hypothetical scenario, Dix asked what would happen to Virginians if there was an administration change and the Attorney General did not prioritize data protection.").

**179.** Press Release, Mark R. Warner, U.S. Sen., Statement of U.S. Sen. Mark R. Warner After Governor Northam Signed Privacy Legislation into Law (Mar. 2, 2021), https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=69CDF4A0-C7E6-4357-A0F1-E9F107FCEF8C [https://perma.cc/HZE2-HW83].

**180.** Moomaw, *supra* note 136.

law, at first providing limited protection to consumers.[181] Hayes has also expressed skepticism about widespread use of facial-recognition technology,[182] noting the problem of higher levels of false positives for people of color and women, bias relating to the use of mug shots, and the importance of avoiding technology that perpetuates racial prejudices.[183] Hayes would eventually like to introduce legislation to address data-privacy concerns related to artificial intelligence and facial recognition.[184] Time will tell whether he can successfully advance legislation of special importance to African Americans through the Virginia state house. Full dismantling of the Black Opticon in the Commonwealth could require demonstrable convergence between the interests of African American Virginians, and the interests of the powerful elites and white majority.[185]

### *D. New Resources for the Federal Trade Commission*

The FTC is without a doubt a major data-privacy regulator. This is true, notwithstanding the limitations of its jurisdiction, authority, and rule-making ability as a consumer and competition protection agency.[186] As Daniel Solove

---

**181.** *See* Jules Pattison-Gordon, *Virgina Privacy Law: Lawmakers Chart Enforcement, Outreach*, GOV'T TECH. (Nov. 9, 2021), https://www.govtech.com/security/virginia-privacy-law-lawmakers-chart-enforcement-outreach [https://perma.cc/G5CZ-RMYU] (describing the politics of the law's passage, Hayes said, "Legislators need a lot of time to fully familiarize themselves with that technology and its implications, which could slow progress on any broader privacy bill that addresses it or see policymakers rejecting the whole thing outright due to concerns over that slice . . . . A simpler bill may leave some goals on the wayside, but legislation that fails to garner the votes it needs leaves behind all goals . . . .").

**182.** Bob Lewis, *Absent a Comprehensive National Strategy, Virginia Considers Tightening Data Privacy and Security Laws*, VA. MERCURY (Sept. 8, 2020, 12:01 AM), https://www.virginiamercury.com/2020/09/08/absent-a-comprehensive-national-strategy-virginia-considers-tightening-data-privacy-and-security-laws [https://perma.cc/KY6X-3NRB].

**183.** *Id.* Some police and sheriff uses of facial recognition are already restricted by legislation in the state. *See* VA. CODE ANN. §§ 59.1-578(A)(4), 15.2-1723.2(A)-(B), 23.1-815.1(A)-(B) (2021). State and airport police use, on the other hand, is still permitted. *See id.* at § 23.1-815.1(C) ("Nothing in this section shall apply to commercial air service airports"). By implication, the statute does not pertain to the private-sector uses of facial recognition technology.

**184.** Cat Zakrzewski, *Virginia Governor Signs Nation's Second State Consumer Privacy Bill*, WASH. POST (Mar. 2, 2021, 8:17 PM EST), https://www.washingtonpost.com/technology/2021/03/02/privacy-tech-data-virgina [https://perma.cc/DG7G-EHAC].

**185.** Insights associated with critical-race theorist Derrick Bell predict that advances in African Americans' interests come when their interests converge with those of white people. *See* Derrick A. Bell, Brown v. Board of Education *and the Interest-Convergence Dilemma*, 93 HARV. L. REV. 518 (1980). Success in *Brown* was possible only because Black and white interests conveniently converged; Black Americans' legal advancement was unlikely in the absence of interest convergence with white people. *Id.* at 523.

**186.** *See* Robert Gellman, *Can Consumers Trust the FTC to Protect Their Privacy?*, ACLU (Oct. 25, 2016, 12:30 PM), https://www.aclu.org/blog/privacy-technology/internet-privacy/can-consumers-trust-ftc-protect-their-privacy [https://perma.cc/X3YM-6Q34] ("1. The FTC has limited jurisdiction. It generally does not have any authority over federal, state, or local agencies; non-profits; banks and insurers; transportation companies; and some other sectors. It cannot serve as a general purpose privacy agency because many institutions that affect consumer privacy fall outside of its authority. 2. The FTC can only address privacy with its general authority to prevent 'unfair or deceptive acts or practices' affecting commerce. The only exception is a small number of areas where Congress gave the agency express

and Woodrow Hartzog observed several years ago, "FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States."[187] The FTC enforces the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, and the Gramm-Leach-Bliley Act,[188] and has undertaken to regulate data breaches, the internet of things, and of special relevance here, online platforms.[189] The Commission's "consumer protection cases involving platforms . . . have also included policing disclosures and controls around in-app purchases by children, deceptive employment opportunity claims made by ride-sharing platforms, revenge-porn, and deceptive use of crowd-funding platforms."[190] The Commission has brought enforcement actions "against many major online platforms, including Twitter, Google, Facebook, Snapchat, and Ashley Madison," alleging that in some of these cases, privacy or security practices were misrepresented to consumers.[191] The FTC does not have a major track record of pursuing enforcement actions against platforms whose unfair or deceptive business practices target consumers belonging to marginalized communities, such as African Americans. This could change as a result of the confluence of three things: continued diverse leadership, dedicated funding for a privacy bureau, and a commitment to addressing the problems of communities of color as a strategic priority.

Diverse leadership at the FTC enhances its capacity to help advance the AAOEA. In September 2021, President Joe Biden nominated Big Tech critic and privacy-law expert Alvaro Bedoya to serve as the Commissioner of the FTC.[192]

---

privacy regulatory authority, as it did for example with the Children's Online Privacy Protection Act. Most privacy cases that the FTC brings rely on its general authority. In fact, most of the cases rely on the deception authority. If a company makes a promise in a privacy policy and fails to carry out that promise, the FTC can act because of the deception. But if a company doesn't promise to protect privacy (and many write vague and unclear privacy policies) there's little the FTC can do even against privacy violations most consumers find offensive. 3.The FTC has no effective general authority to issue privacy regulations beyond a few specific statutes. Decades ago, the FTC was more aggressive in other areas, and the Congress (in the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act of 1975) placed severe limits on the FTC's authority so that new regulations are nearly impossible.").

187. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585-86 (2014). The authors pointed out that "[s]ince the late 1990s, the Federal Trade Commission . . . has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices. The FTC has also been enforcing several privacy statutes and . . . [agreements] that enable[] companies to transfer data between the United States and the European Union." *Id*.

188. *Id.* at 643-47.

189. *See* Terrell McSweeny, *FTC 2.0: Keeping Pace with Online Platforms*, 32 BERKELEY TECH. L.J. 1027, 1035-36 (2017); Kathleen A. Murphy, *Recent FTC Regulation of the Internet of Things*, 73 BUS. LAW. 289 (2017); Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008).

190. McSweeny, *supra* note 189, at 1035 (footnotes omitted).

191. *Id.* at 1036.

192. *See* Press Release, White House, President Biden Announces 10 Key Nominations (Sept. 13, 2021), https://www.whitehouse.gov/briefing-room/statements-

He was the Founding Director of the Center on Privacy and Technology at Georgetown University Law Center, and a former Chief Counsel of the U.S. Senate Judiciary Subcommittee on Privacy, Technology and the Law.[193] An immigrant from Peru and naturalized U.S. citizen, Mr. Bedoya has demonstrated an understanding of the problem of racial-minority-targeting surveillance.[194] Mr. Bedoya's expertise could increase the effectiveness of the Commission with respect to identifying privacy concerns, setting priorities, and enforcing privacy laws.

The possibility of major congressional funding for a new FTC privacy division emerged in September 2021. The U.S. House Committee on Energy and Commerce voted to appropriate $1 billion to "create and operate a bureau to accomplish the work of the Commission related to unfair or deceptive acts or practices relating to privacy, data security, identity theft, data abuses, and related matters."[195] The proposed appropriation would be available to the FTC in 2022 and remain available until September 30, 2031 for carrying out these purposes.[196] The new division would have the resources to aggressively punish unfair trade practices and vigorously enforce laws enacted by Congress. With the mandate to address "data abuses," the new division would seem to have an enlarged capacity to attack discriminatory exclusion and scamming targeting African Americans—already a stated FTC priority.[197] Were the proposed division to materialize, resources could be made available to enforce privacy laws with an unprecedented race-conscious zeal, as called for in the African American Online Equity Agenda. Indeed, some commentators argue that—with increased legal authority, funding, and more technologists—a new privacy division within the FTC would "not just protect 'privacy,' but would also address broader data protection concerns, including anticompetitive data practices and the use of data for fraud, racial profiling, and discrimination."[198]

The FTC already has a race-conscious antidiscrimination agenda that could be pivoted to focus more specifically on improving online equity for people of color. In 2014, the agency established its "Every Community Initiative" to "modernize and expand the agency's work and to develop a strategic plan for

---

releases/2021/09/13/president-biden-announces-10-key-nominations-2 [https://perma.cc/J6LU-6U6X]; David McCabe, *Biden Will Name a Privacy Expert to Federal Trade Commission*, N.Y. TIMES (Sept. 13, 2021), https://www.nytimes.com/2021/09/13/technology/Alvaro-Bedoya-ftc.html [https://perma.cc/SB5V-QTYE].

193. Press Release, *supra* note 192.

194. *See* Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016) (exposing the extent of facial-recognition AI in use in the United States).

195. *See* H.R. 5237, 117th Cong. § 31501 (2021).

196. *Id.* at 1.

197. *See Combatting Fraud in African American & Latino Communities: The FTC's Comprehensive Strategic Plan*, FED. TRADE COMM'N 15 (June 15, 2016) [hereinafter *Combatting Fraud*], https://www.ftc.gov/system/files/documents/reports/combating-fraud-african-american-latino-communities-ftcs-comprehensive-strategic-plan-federal-trade/160615fraudreport.pdf [https://perma.cc/RNV3-YLTP]; FED. TRADE COMM'N, *supra* note 9, at 3.

198. Jessica Rich, *Five Reforms the FTC Can Undertake Now to Strengthen the Agency*, BROOKINGS INST. (Mar. 1, 2021), https://www.brookings.edu/blog/techtank/2021/03/01/five-reforms-the-ftc-can-undertake-now-to-strengthen-the-agency [https://perma.cc/L8Y6-JF6M].

addressing disparities and other issues affecting communities of color."[199] In June 2016, the agency released a congressionally mandated report, *Combatting Fraud in African American & Latino Communities: The FTC's Comprehensive Strategic Plan*, which reported on the outcomes of a "strategy to reduce fraud in Black and Latino communities . . . summarizing the FTC's relevant law enforcement work as well as its targeted consumer outreach and education initiatives."[200] The report described an instance of race discrimination as measured through one of its enforcement actions: the victims of a payday-loan and bank scam were four times as likely to be African American than white or Hispanic.[201]

In 2021, the FTC released a second report, *Serving Communities of Color*, which describes the Commission's "strides in addressing fraud in Black and Latino communities" and "expanded . . . efforts to include other communities of color such as Asian American and Native American communities, and other non-fraud related consumer issues that also disproportionately affect communities of color."[202] The report identifies specific contextual harms experienced by Asian American, Latinos, and African Americans.[203] And it explains that the FTC, which emphasizes the importance of education and outreach in addition to enforcement actions,[204] has brought about two dozen actions involving conduct specifically targeting or disproportionately impacting communities of color.[205]

Plaudits go to the Commission both for recent efforts at delineating harms specific to designated racial groups comprising marginalized communities and for its readiness to allocate resources to addressing them, now and in the future. From the vantage point of the African American Online Equity Agenda, the next step would be to focus more investigations and enforcement actions on allegations of online and platform-related fraud, deception, and unfair trade practices disproportionately affecting and targeting peoples of color.

Diverse leadership, additional funding, and stated priorities do not change the jurisdiction and authority of the FTC, which was founded about 108 years ago to combat fraud, deception, and unfair business practices.[206] The agency has not been authorized to serve as an all-purpose national online privacy and

---

**199.** FED. TRADE COMM'N, *supra* note 9, at 1.

**200.** *Id.*

**201.** FED. TRADE COMM'N, *supra* note 197, at 15 (analyzing data from a case in which defendants "placed unauthorized debits" on the bank accounts of consumers who had once applied for payday loans).

**202.** FED. TRADE COMM'N, *supra* note 9, at 1.

**203.** *Id.* at 1-2.

**204.** *Id.* at 23-35.

**205.** *Id.* at 1.

**206.** *See Our History*, FTC, https://www.ftc.gov/about-ftc/our-history [https://perma.cc/VT9N-EP7S ] (stating that the FTC was founded in 1914 to protect consumers and promote competition).

data-protection regulator.[207] Some platform problems characteristic of the Black Opticon may be beyond its current reach. Platform companies' uses of artificial intelligence pose some of platform privacy's biggest challenges, and those uses can be discriminatory or unfair to people of color and other consumers.

In a recent book examining the "investigative gaze" of businesses and governments,[208] Robert H. Sloan and Richard Warner propose that an expanded FTC or "FTC-like" regulatory agency be "politically empowered and adequately funded with significantly expanded powers to make and enforce judgments of fairness" about whether uses of AI operate on a level playing field.[209] Although they argue that it is plausible to think the FTC could regulate AI, Sloan and Warner do not make the case that Congress should in fact explicitly expand the jurisdiction of the FTC to allow for broad regulation of business uses of AI.[210] Nor do Sloan and Warner take on the issue whether the FTC would begin to impose meaningfully large monetary fines on Big Tech, were violations found to have occurred under the expanded interpretation of FTC's authority they propose.[211] Expanded FTC jurisdiction pursuant to its investigatory, law-enforcement, and rule-making powers is not on the horizon, which fuels interest in an independent federal data-protection agency.

### *E. A Proposed Federal Data-Protection Agency*

Now that we are in a digitally dependent age with a thoroughly digital economy, we cannot depend solely upon existing law enacted decades ago. We

---

**207.** *See* Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2018). The FTC describes itself as a law-enforcement agency having responsibilities for consumer protection and the promotion of competition. *Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement [https://perma.cc/66J9-XZHS] ("FTC enforces federal consumer protection laws that prevent fraud, deception and unfair business practices. The Commission also enforces federal antitrust laws that prohibit anticompetitive mergers and other business practices that could lead to higher prices, fewer choices, or less innovation."); *see A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (May 2021), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/VEV6-3CTJ].

**208.** *See* ROBERT H. SLOAN & RICHARD WARNER, THE PRIVACY FIX: HOW TO PRESERVE PRIVACY IN THE ONSLAUGHT OF SURVEILLANCE 1, 22-42, 181-203 (2021) (relating "artificial intelligence"—defined as roughly synonymous with "predictive analytics" and "machine learning"—to privacy-diminishing surveillance); Tyler Becker, *When Congress Makes No Policy Choice: The Case of FTC Data Security Enforcement*, 120 COLUM. L. REV. 134, 134-52 (2020) (raising jurisdictional issues respecting data-breach enforcement under the unfairness and deceptive prongs of Section 5). *See generally* ZUBOFF, *supra* note 19 (detailing aspects of the "black box" online and platform economy that disadvantage users and the general public); PASQUALE, *supra* note 4 (same).

**209.** SLOAN & WARNER, *supra* note 207, at 199.

**210.** The agency has enforcement roles respecting Gramm-Leach Bliley, the Children's Online Privacy Protection Act (COPPA), and other federal privacy laws. Its most recent budget request for about $490 million did not include funding for novel or expanded privacy-law enforcement activities. *Cf.* Rebecca Kelly Slaughter, *Congressional Budget Justification Fiscal Year 2022*, FED. TRADE COMM'N (May 28, 2021), https://www.ftc.gov/system/files/documents/reports/fy-2022-congressional-budget-justification/fy22cbj.pdf [https://perma.cc/8T46-GTHD].

**211.** *See* PASQUALE, *supra* note 4, at 213 (pointing out that a "record-setting" $22.5 million fine imposed by the FTC on Google represented only four hours of Google revenue).

need new federal legislation. Were landmark twenty-first century privacy legislation to follow the lead of the Privacy Act of 1974—the federal statute regulating access to personal information held in federal government records and one of the first federal statutes specifically dedicated to information-privacy protection—it would be accompanied by findings and purposes.[212] Preambles of finding and purpose accompanying congressional legislation inform the public about the issues that have led Congress to enact new law. They explain "what Congress hoped to achieve in enacting the legislation."[213] The Privacy Act of 1974's findings included that the use of computer technology and the misuse of information systems can expose individuals to serious practical harms, and that the right to privacy is a constitutionally protected personal and fundamental right.[214]

Since 1974, harms associated with information technology have multiplied in number and severity. Congress might have found in 1974, as it could today, that privacy is a basic human right of international stature and a civil right.[215] Unlike in 1974, Congress could today find that the right to privacy and related rights of data protection are deeply embedded in numerous state and federal statutes and in the basic law and statutes of jurisdictions around the world.[216] New legislation could include findings that harms attributed to online platforms include some that disproportionately affect people of color burdened by racism and prejudice.[217] In addition, the findings could reiterate that the ability to obtain and enjoy privacy is affected by structures of class, race, power, and privilege that the design of new law must address in the interest of equity and civil rights.[218] In short, the findings of a new comprehensive federal privacy law could and should incorporate the assumptions of the AAOEA: privacy is unequally distributed; well-meaning privacy laws may have disparate impacts; and African Americans are especially vulnerable to data-privacy-related oversurveillance, exclusion, and predation. Including such findings would signal awareness of the special vulnerabilities of African Americans, educate those reading the law about that vulnerability, and prepare the public for provisions

---

**212.** *See* Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)-(b), 88 Stat. 1896, 1896 (codified as amended at 5 U.S.C. § 552a (2018)) (illustrating findings and purposes).

**213.** Jarrod Shobe, *Enacted Legislative Findings and Purposes*, 86 U. CHI. L. REV. 669, 671 (2019).

**214.** *See* Privacy Act of 1974 § 2(a), 88 Stat. at 1896.

**215.** *Cf.* Anita L. Allen, *Natural Law, Slavery, and the Right to Privacy Tort*, 81 FORDHAM L. REV. 1187, 1210-15 (2012) (relating goals of protection in U.S. common law to international and European Union privacy standards).

**216.** MARC ROTENBERG, PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW AND RECENT DEVELOPMENTS (2020); Commission Regulation 2016/679, 2016 O.J. (L 119) 1; Personal Information Protection Law (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (China); Personal Data Protection Act 2012 (No. 26 of 2012) (Sing.).

**217.** NOBLE, *supra* note 31.

**218.** *See generally* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGIN (2020) (advocating for new legal norms that "will better advance the privacy rights of marginalized communities in courts and society").

of new laws that referred to marginalized groups such as African Americans or drew upon the discourse of civil rights. A number of bills aimed at privacy protection were introduced into the 116th and 117th Congresses, none with preambles stating intentions to combat racial disparities as such.[219] But an examination of the provisions of legislation introduced by Senator Kristen Gillibrand reveals equitable intentions and the potential for measures specifically responsive to the guidance of the AAOEA.

In June 2021, Senator Gillibrand, joined by cosponsor Senator Sherrod Brown, introduced the Data Protection Act of 2021 (DPA).[220] Their bill would create an autonomous federal Data Protection Agency (FDPA) headed by a presidentially appointed director,[221] decreasing dependence on the FTC for privacy-law enforcement. Whether the nation would need both an FTC privacy bureau and a general-purpose data-protection agency is unclear, since their precise parameters are not fully determined. But the bill does not presuppose major changes at the FTC and it would create durable institutional structures and mechanisms for realizing major reforms. Through the roles the DPA assigned its three divisions, the FDPA would enable consequential policy making, research, and law enforcement; protect against privacy harms and discrimination; oversee data practices; and propose remedies for the adverse social, ethical, and economic implications of data practices.[222] The bill would also enable efforts to address what a Brookings Report refers to as high complexity, low consensus "hard issues"— namely, limits on data processing, algorithmic transparency, and algorithmic fairness.[223]

The Gillibrand-Brown proposal was unique among the several bills introduced in the 116th and 117th Congresses by other members. It alone called for the creation of a FDPA with a Civil Rights Office to "regulate high-risk data practices and the collection, processing, and sharing of personal data."[224]

---

**219.** *Cf.* Müge Fazlioglu, *U.S. Federal Privacy Legislation Tracker*, INT'L ASS'N PRIV. PROS., https://iapp.org/resources/article/us-federal-privacy-legislation-tracker [https://perma.cc/ZC53-4T5V]; *see also* Müge Fazlioglu, *Privacy Bills in the 117th Congress*, INT'L ASS'N OF PRIV. PROS (Aug. 24, 2021), https://iapp.org/news/a/privacy-bills-in-the-117th-congress [https://perma.cc/5VCY-P8AQ] (identifying and comparing content of bills introduced into Congress).

**220.** *See* Data Protection Act of 2021, S. 2134, 117th Cong (2021).

**221.** *See id.* at §§ 3(b)(1), 4(d) (relating to the presidential appointment of the Director and to agency autonomy, respectively).

**222.** *Id.* at § 5(b)(1)-(3).

**223.** *See* Cameron F. Kerry, John B. Morris, Jr., Caitlin T. Chin & Nicol E. Turner Lee, *Bridging the Gaps: A Path Forward to Privacy Legislation*, BROOKINGS INST. 12 (June 2020), https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf [https://perma.cc/JUJ9-WCZD].

**224.** S. 2134 § 3(a); *see also* JONATHAN M. GAFFNEY, CONG. RSCH. SERV., LSB10441, WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS 1-2 (2020) ("Five of the six proposals—H.R. 4978, S. 2968, S. 3456, and the two discussion drafts—take similar approaches. Although details vary somewhat from bill to bill, each regulates the use of personal information by: (1) recognizing individuals' rights to control their personal information; (2) requiring a defined class of entities to take steps to respect those rights; and (3) creating procedures to enforce those requirements. The five proposals differ, however, in three key respects: (1) which federal agency would have enforcement power; (2) whether to preempt state privacy laws; and (3) whether to provide a private right of action. The sixth bill, S. 3300, takes a different approach: it would create a new agency vested with the power to enforce existing federal privacy laws and authorize that agency to issue broadly applicable privacy regulations.").

The definition of "high-risk" data practices reveals a specific (though implicit) legislative purpose to attack the Black Opticon. The bill defines a "high-risk data practice" to include an action by a data aggregator that involves: automated decision systems; data-respecting protected-class status, income, and criminal convictions; access to services, products, and opportunities; systematic processing of publicly accessible data on a large scale; profiling of individuals on a large scale; children, youth, and the elderly; people with disabilities; and geolocation processing.[225] The "high-risk" data practices of particular concern to the statute are those of commercial data aggregators, defined as "any person that collects, uses, or shares, in or affecting interstate commerce, an amount of personal data that is not de minimis, as well as entities related to that person by common ownership or corporate control."[226] Big Tech platforms meet the definition of data aggregators, since they collect, use, or share more than nominal amounts of personal data in interstate commerce; their data practices would therefore fall under the purview of the FDPA.[227]

The FDPA would have the power to conduct investigations of possible violations, issue subpoenas, grant injunctive relief and equitable remedies, and, critically, impose civil penalties and fines.[228] Fines of $3 million per day could deter large and small tech firms more effectively than penalties currently levied by the FTC.[229] A portion of fees and assessments would be placed in a "Data Protection Agency Fund" to support agency activities.[230] To foster greater accountability to the public, the Act would mandate soliciting reports and examinations from large data aggregators, as well as agency review of mergers of large data aggregators or mergers involving the transfer of personal data of over 50,000 persons, and reports to the FTC and Department of Justice on the privacy implications of such mergers.[231]

---

**225.** S. 2134 § 2(11) (defining "high-risk data practice").

**226.** *Id.* § 2(6)(A) (defining "data aggregator"). An exception in § 2(6)B clarifies that data collection for noncommercial purposes is not covered by the statute.

**227.** *Id.* § 2(6)(A).

**228.** *Id.* § 13(e)(3)(b) (describing penalty amounts).

**229.** *Id.* § 8(d)(1) (establishing a Civil Penalty Fund); *id.* § 13(e)(3)(B)(iii)(I)-(II) (listing fines of up to $1,000,000 and $3,000,000 per day for knowing violations of the statute or any privacy law); *see also* Christine S. Wilson, Comm'r, U.S. Fed. Trade Comm'n, A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Regulation, Remarks at the Future of Privacy Forum (Feb. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf [https://perma.cc/8W23-DBNV] (identifying strengths and weaknesses in the FTC's ability to address the full range of privacy problems); *cf.* Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, But Not Without Help from Congress*, BROOKINGS INST. (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress [https://perma.cc/AF6U-DTV9] (arguing that the FTC requires legislative help from Congress to effectively regulate technology companies).

**230.** *See* S. 2134 § 8(d)(2) (payments to victims).

**231.** *Id.* § 11(b) (large-aggregator reporting); *id.* § 11(d) (merger-related reporting).

Of course, creating a new agency costs money and takes time.[232] But in the past, "Congress has repeatedly created new departments and new administrative agencies to meet problems arising as the nation and its economy matured."[233] The digital economy presents a serious set of problems for modern life that warrants a new administrative agency. The challenges posed by platform regulation are broad ranging, highly technical, and implicate core civil rights and civil liberties. The need to design and enforce nimble platform regulation stands among the reasons why the United States should take seriously the possibility of creating a specialized agency.[234]

Senator Gillibrand's DPA is not likely to move through Congress soon or intact, but when and if it eventually does, some of its current provisions could become law. Setting a high bar for future legislative-reform proposals, the Gillibrand Act is striking for its deep responsiveness to calls for *equitable* platform-privacy governance. In the past thirty years, equity has not been a clear top priority of privacy legislation. The Act signals a new era, laying out a dynamic framework for an agency with unprecedented authority to pursue equity in the context of data protection through all three of its major units: Civil Rights, Research, and Complaints.[235] Through its three functional divisions, the FDPA would have the authority to enforce new data-protection rules enacted by Congress or promulgated by the agency itself.

The protection of civil rights is increasingly recognized as an important component of privacy and data-protection laws, as evidenced by recently proposed federal privacy and data-protection statutes that contain nondiscrimination provisions.[236] The protection of civil rights needed to address

---

**232.** Still, despite the required work and expense, following the financial crisis of 2008 and subsequent major recession, in 2010, Congress created the Bureau of Consumer Financial Protection pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified as amended at 12 U.S.C. §§ 5491-5497 (2018)). The Bureau has been plagued by partisan politics. *See* Gail Whittemore, *Controversy over the Consumer Financial Protection Agency*, PACE L. LIBR. (Apr. 20, 2018), https://lawlibrary.blogs.pace.edu/2018/04/20/controversy-over-the-consumer-financial-protection-bureau [https://perma.cc/7RM8-SZLL].

**233.** Peter L. Strauss, *How the Administrative State Got to This Challenging Place*, 150 DAEDALUS J. AM. ACAD. ARTS & SCI. 17, 18 (2021).

**234.** *See id*. at 18-23.

**235.** *See* S. 2134 § 5(b)(1)-(3).

**236.** For example, in 2019 Senator Maria Cantwell, a Democrat from Washington, introduced a Consumer Online Privacy Rights Act. *See Cantwell, Senate Democrats Unveil Strong Online Privacy Rights*, MARIA CANTWELL (Nov. 26, 2019), https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights [https://perma.cc/KSF4-P8HQ]. The Act would prohibit "covered entities" from transferring or processing data "on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability . . . in a manner that unlawfully segregates, discriminates against, or otherwise makes available to the individuals or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation." Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 108 (2019). The proposed law's civil-rights section also requires "Algorithmic Decision-making Impact Assessments" where algorithms are used to facilitate "decisionmaking relating to eligibility determination for housing, educations, employment or credit opportunities." *Id.* at § 108(b)(1). A bill introduced by Senator Roger Wicker, a Republican from Mississippi, in July 2021 would empower the FTC to offer enforcement

the Black Opticon is manifest in the provision that the FDPA's Office of Civil Rights would "ensure that the collection, processing, and sharing of personal data is fair, equitable, and non-discriminatory in treatment and effect."[237] The civil-rights equity goal is manifest in the provision that the Office of Civil Rights would aim at promoting the traditional civil-rights goal of equal opportunity through responsibility for "developing, establishing, and promoting data processing practices that affirmatively further equal opportunity to and expand access to housing, employment, credit, insurance, education, healthcare, and other aspects of interstate commerce."[238] Recognizing the importance of coordination and connection, the Office would "coordinate[] the Agency's civil rights efforts with other Federal agencies and State regulators . . . to promote consistent, efficient, and effective enforcement of Federal civil rights laws";[239] would "work[] with civil rights advocates, privacy organizations, and data aggregators on the promotion of compliance with the civil rights provisions under this Act, rules and orders promulgated under this Act, and Federal privacy laws";[240] and would "liaise[] with communities and consumers impacted by practices regulated by this Act and the Agency, to ensure that their needs and views are appropriately taken into account."[241] The DPA defines "protected class" as "the actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender identity or expression, sexual orientation, familial status, biometric information, genetic information, or disability of an individual or a group of individuals."[242] The Office of Civil Rights would be empowered to investigate claims that members of a protected class are disadvantaged by platform practices or policies, such as a ban-optic advertisement-purchasing platform that prevented African American persons from viewing certain advertisements.[243]

The Act also establishes a Research unit whose responsibilities manifestly promote the ideal of equitable data policies and practices on online platforms. This unit would support enactment of comprehensive, well-informed, and equitable federal information-privacy laws. Research-unit responsibilities

---

assistance in the form of information transmissions to other authorities when "[a] covered, entity, service provider, or third party" acts to "collect, process, or cover data in violation of Federal civil rights laws."). *See* Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act, S. 2499, 117th Cong. § 201(a)-(b) (2021).

**237.** S. 2134 § 5(b)(1)(A).

**238.** *Id.* § 5(b)(1)(B).

**239.** *Id.* § 5(b)(1)(C).

**240.** *Id.* § 5(b)(1)(D).

**241.** *Id.* § 5(b)(1)(E).

**242.** *Id.* § 2(21).

**243.** *Cf.* Katie Paul & Akanksha Rana, *U.S. Charges Facebook with Racial Discrimination in Targeted Housing Ads*, REUTERS (Mar. 19, 2019), https://www.yahoo.com/now/hud-charges-facebook-housing-discrimination-115928711.html [https://perma.cc/H2YR-NPGK] (reporting that Facebook allegedly sold targeted advertising that discriminated against certain groups by "restrict[ing] who could see housing-related ads based on national origin, religion, family status, sex, and disability").

would include "researching, analyzing, assessing, and reporting" relating not only to "the collection and processing of personal data" and "the collection and processing of personal data by government agencies, including contracts between government agencies and data aggregators,"[244] but also "unfair, deceptive, or discriminatory outcomes that result or are likely to result from the use of automated decision systems, including disparate treatment or disparate impact on the basis of protected class or proxies for protected class."[245] Staffed with data scientists and privacy-law experts, the Research unit would be charged with measuring the costs and benefits of "high-risk data practices," which includes identifying their unintended consequences and assessing their potential disparate impacts and privacy harms.[246] The Research unit's mandate would go to the heart of concerns about the harms that stem from online platforms and disproportionately impact African Americans or others in protected classes. The Act defines "privacy harms" broadly to include economic, physical, and emotional harms.[247] The threats and harassments people of color face online would appear by definition to count as physical harms, and the burdens of anxiety and stigma would count as emotional harms.

Further, with an ear to the ground, through the Complaint unit, the DPA would have the capacity to quickly identify and address online platform inequities. The Complaint unit within the new agency would be dedicated to collecting and tracking grassroot consumer complaints made by telephone or on a website. Incentivizing resort to the new agency, a "Data Protection Civil Penalty Fund" would be available to compensate individual and classes of victims of federal privacy-law violations.[248]

Through the design of the FDPA and its allocated responsibilities, the Act boldly rejects some experts' tepid approach to civil-rights issues related to privacy governance.[249] Viewed through the lens of race, Senator Gillibrand's 2021 reform proposal merits praise. It prioritizes the ability of the federal government to respond to the documented racial bias against African Americans and other vulnerable groups through an equity-conscious and protected class-conscious FDPA comprised of a trio of civil-rights, research, and complaint-gathering units. The proposed Office of Civil Rights could prove

---

**244.** S. 2134 § 5(b)(2)(A)-(B).

**245.** *Id.* § 5(b)(2)(C).

**246.** *Id.* § 2(11)-(13).

**247.** *Id.* § 2(18).

**248.** *Id.* § 8(d)(1) (Civil Penalty Fund).

**249.** *See, e.g.*, Kerry et al., *supra* note 222, at 14 ("Civil Rights: Existing federal anti-discrimination laws, designed for human decision-making, need reinforcement to address automated decisions. Comprehensive privacy legislation should address algorithmic discrimination because covered data can be used in ways that disadvantage individuals. However, privacy legislation should not alter existing federal or state anti-discrimination laws, and the agencies currently tasked with anti-discrimination enforcement (e.g., the EEOC) should maintain their primary roles. The FTC should refer discrimination cases to the relevant federal agency, and privacy legislation should also prohibit the use of covered data in ways that violate existing anti-discrimination laws.").

especially critical to addressing disparate impacts and racial bias in algorithms and automated decision-making systems.[250]

Enthusiasm for the high bar set by the Act must be tempered by realism. It is uncertain what it will take for the DPA to go from proposal to reality and when. Within the United States, comprehensive federal legislation will require that Congress resolve issues of overlap, duplication, and preemption that will multiply as other states follow the lead of Virginia, California, and Colorado—and as the FTC potentially pushes ahead to establish its own in-house privacy bureau.

In addition, while features of the DPA discussed in this Section should enable meaningful measures to address platform equity concerns raised by people of color, it is not a cure for all of the unfounded surveillance, AI disparities, and exclusion and exploitation experienced by Black people online. The Act might hold platform firms more responsible to noxious content, but it cannot force racially biased platform users to leave people of color alone and regard fellow users with equal respect. No law can. And the Act does not, of course, address offline law-enforcement abuses. The Act might demand limits on uses by the public sector of facial-recognition technologies and biometrics, but it cannot prevent racism-related discretionary uses of force by police on the ground that violate expectations of privacy.

## conclusion

Simone Browne innovated "the concept of racializing surveillance," defined as "a technology of social control where surveillance practices, policies, and performances concern the production of norms pertaining to race and exercise of 'a power to define what is in or out of place.'"[251] Digital platforms are racializing technologies in this sense. Despite some scholars' rejection of the panopticon metaphor that it enfolds,[252] the Black Opticon is a useful, novel rubric for characterizing the several ways African Americans and their data are subject to pernicious forms of discriminatory attention by racializing technology online. Online attention can work to keep Black people in an historic place of social and economic disadvantage.

Digital society and online platforms "reinforce and reproduce racist social structures" through "software, policies, and infrastructures that amplify hate,

---

**250.** *See* Press Release, Color of Change, Civil Rights Coalition Releases Core Principles on Civil Rights and Privacy Online, https://colorofchange.org/press_release/civil-rights-coalition-releases-core-principles-ci [https://perma.cc/62MT-NAHK] (framing data-privacy issues as civil-rights issues); Harrison, *supra* note 84.

**251.** SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 16 (2015) (quoting OSCAR GANDY, THE PANOPTIC SORT: THE POLITICAL ECONOMY OF PERSONAL INFORMATION 15 (1993)).

**252.** *See id.* at 38-50 (discussing scholars who reject the panopticon metaphor).

racism, and white supremacy."[253] They cause social harms such as privacy loss, political harms such as threatening democratic discourse and choice, as well as the abuse of economic power.[254] Platforms could in theory use their resources voluntarily to counteract these abuses.[255] Instead Big Tech struggles with self-governing its platforms to deal with racist content and discrimination in opportunity, services, and privacy. They gesture at change more than fundamentally change. The paucity of people of color in management and leadership positions in Silicon Valley worsens the situation since their absence excludes "advanced-degree holders [in ethnic studies] . . . with deep knowledge of history and critical theory."[256]

This Essay advocates for treating some of the ills affecting African Americans on online platforms with privacy and data-protection reforms, while recognizing that the complete remedy demands "a coordinated and comprehensive response from governments, civil society and the private sector."[257] I believe the Black Opticon of panoptic, ban-optic, and con-optic discrimination is amenable to attack by well-designed, race-conscious legal reform. Which of the three pillars of the Black Opticon will prove most amenable to destruction through privacy law is an open question I have not attempted to answer here.

Racially equitable policies and aspirations emerge to varying degrees in proposed and enacted privacy and data-protection law, such as the VCDPA, the proposed FTC privacy bureau, and the proposed federal data-protection agency. These reform agendas have a grave purpose, as grave as the purposes that motivated the twentieth-century civil-rights movements. Understandings of the specific impact of diminished data privacy and inadequate data protection on African Americans will continue to unfold. But in the meantime, we should consciously seek to regulate platforms—and, indeed, all of the digital economy—with an agenda that centers nondiscrimination, antiracism, and antisubordination on behalf of African Americans.[258]

---

**253.** Bharath Ganesh, *Platform Racism: How Minimizing Racism Privileges Far Right Extremism*, SOC. SCI. RSCH. COUNCIL NETWORK ITEMS (Mar. 16, 2021), https://items.ssrc.org/extremism-online/platform-racism-how-minimizing-racism-privileges-far-right-extremism [https://perma.cc/N2VQ-VWAJ]; *see also* NOBLE, *supra* note 31, at 10, 28 (arguing that "intersectional power analysis" underscores that algorithms "reinforce oppressive social and economic relationships").

**254.** *See* Francis Fukuyama, Barak Richman, Ashish Goel, Roberta R. Katz, A. Douglas Melamed & Marietje Schaake, *Report of the Working Group on Platform Scale*, STAN. CTR. ON PHILANTHROPY & CIV. SOC'Y 2-3 (2020), https://pacscenter.stanford.edu/wp-content/uploads/2020/11/platform_scale_whitepaper_-cpc-pacs.pdf [https://perma.cc/LAF9-73Q3].

**255.** *See id*. at 6.

**256.** NOBLE, *supra* note 31, at 163. I am assuming that a majority of Black, Latinx, Asian, and Native American studies college graduates are people of color.

**257.** Owen, *supra* note 16, at 416; *cf. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. OF ECON. COOP. & DEV. (1980), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/S3R9-US9U] ("[T]he problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level.").

**258.** *Cf.* SKINNER-THOMPSON, *supra* note 215, at 6 (discussing an antisubordination approach to privacy law designed to inclusively promote the interests of marginalized groups, including African Americans).

*I would like thank the* Yale Law Journal*, the Information Society Project and the Knight Foundation for publishing the innovative series* Envisioning Equitable Online Governance*, that includes my Essay. I would like to express gratitude to Professors Christopher Yoo, Cary Coglianese, Niva Elkin-Koren, Tamar Kricheli-Katz and Ezekiel Dixon-Roman for encouraging this Essay and giving me platforms on which to share its ideas. I thank Jeramie Scott, Senior Counsel at the Electronic Privacy Information Center (EPIC) for early guidance on looking at privacy through the lens of race, and my trusted Penn research assistants, Alexander Mueller and Matthew Brotz. Finally, my very special thanks go to Roman Leal for his extraordinary patience in guiding me through the editorial process at the* Yale Law Journal*.*