Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice

Michele E. Gilman*

ABSTRACT

Algorithmic profiling technologies are impeding the economic security of low-income people in the United States. Based on their digital profiles, low-income people are targeted for predatory marketing campaigns and financial products. At the same time, algorithmic decision-making can result in their exclusion from mainstream employment, housing, financial, health care, and educational opportunities. Government agencies are turning to algorithms to apportion social services, yet these algorithms lack transparency, leaving thousands of people adrift without state support and not knowing why. Marginalized communities are also subject to disproportionately high levels of surveillance, including facial recognition technology and the use of predictive policing software.

American privacy law is no bulwark against these profiling harms, instead placing the onus of protecting personal data on individuals while leaving government and businesses largely free to collect, analyze, share, and sell personal data. By contrast, in the European Union, the General Data Protection Regulation (GDPR) gives EU residents numerous, enforceable rights to control their personal data. Spurred in part by the GDPR, Congress is debating whether to adopt comprehensive privacy legislation in the United States. This article contends that the GDPR contains several provisions that have the potential to limit digital discrimination against the poor, while enhancing their economic stability and mobility. The GDPR provides the following: (1) the right to an explanation about automated decision-making; (2) the right not to be subject to decisions based solely on automated profiling; (3) the right to be forgotten; (4) opportunities for public participation in data processing programs; and (5) robust implementation

---

* Venable Professor of Law and Director, Saul Ewing Civil Advocacy Clinic, University of Baltimore School of Law; Faculty Fellow, Data & Society. B.A., Duke University; J.D., University of Michigan Law School. Many thanks for feedback to the researchers at Data & Society and the faculties of William & Mary Law School, Pace Law School, and Drexel University School of Law.

and enforcement tools. The interests of low-income people must be part of privacy lawmaking, and the GDPR is a useful template for thinking about how to meet their data privacy needs.

I. INTRODUCTION

On May 18, 2018, citizens of the European Union awoke to a new, robust set of data privacy protections codified in the General Data Protection Regulation (GDPR), which gives them new levels of control over their

personal information.[1] Meanwhile, Americans rise daily to the same fragmented privacy regime that has failed to forestall a drumbeat of data breaches, online misinformation campaigns, and a robust market in the sale of personal data, usually without their knowledge.[2] For instance, in 2017, the credit reporting company Equifax disclosed that hackers had breached its servers and stolen the personal data of almost half the United States's population.[3] In 2018, we learned that Cambridge Analytica harvested the data of over 50 million Americans through personality quizzes on Facebook in order to target voters with political advertisements for the Trump campaign.[4] And, as consumers are bombarded with advertisements based on their internet searches or remarks captured by digital assistants such as Amazon's Alexa, Americans are increasingly realizing that their online and offline behavior is being tracked and sold as part of a massive, networked data-for-profit and surveillance system.[5]

The American privacy regime is largely based on a notice and consent model that puts the onus on individuals to protect their own privacy.[6] The model is not working. In the absence of congressional action, some states have enacted laws to protect the data privacy and/or security of their citizens.[7] California has enacted the most comprehensive statute, effective January 2020, entitled the California Consumer Privacy Act, which expands transparency about the big data marketplace and gives consumers the right to opt-out of having their data sold to third parties.[8] Other states may soon

---

1. Commission Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter GDPR].

2. *See* SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 353–55 (2018).

3. Stacy Cowley, *2.5 Million More People Potentially Exposed in Equifax Breach*, N.Y. TIMES (Oct. 2, 2017), https://www.nytimes.com/2017/10/02/business/equifax-breach.html [https://perma.cc/8VWZ-L653].

4. Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline [https://perma.cc/9LVD-9DAG].

5. Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ [https://perma.cc/8WLL-QL4Y].

6. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882–83 (2013).

7. *State Laws Related to Internet Privacy*, NAT'L CONF. ST. LEGISLATURES (Jan. 27, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#Consumer [https://perma.cc/68V2-C338].

8. CAL. CIV. CODE § 1798.100 (West 2020). For more analysis of the California Consumer Privacy Act, see *infra* Part IV.

follow suit. After years of resistance, Big Tech companies such as Facebook, Google, Microsoft and Apple are now advocating for a national data protection law, primarily because they are worried about the emergence of varying state standards.[9] Moreover, Big Tech is already working to comply with the GDPR for their millions of European consumers.[10] In light of these new laws and the American public's "techlash" against revelations of big data scandals,[11] Congress is finally and seriously considering comprehensive privacy legislation.[12] While the issue has bipartisan support, proposals vary in their solicitude for corporations versus consumers.[13] As these issues are being actively debated, it is essential that the legislative process include the interests of all Americans, and not just elites and industry.

Simply put, digital privacy needs are not the same for all Americans. Based on their digital profiles, low-income people are targeted with marketing campaigns for predatory products such as payday loans and for-profit educational scams.[14] At the same time, algorithmic decision-making can result in their exclusion from mainstream employment, housing, financial, and educational opportunities.[15] Government agencies are turning to algorithms to apportion public benefits, yet these automated decision-making systems lack transparency, leaving thousands of people adrift without state support and not knowing why.[16] Marginalized communities are also subject to high levels of law enforcement surveillance, including the use of

---

9. *See, e.g.*, Ben Brody & Spencer Soper, *Amazon Joins Tech Giants in Backing Federal Privacy Safeguards*, BLOOMBERG (Sept. 26, 2018), https://www.bloomberg.com/news/articles/2018-09-26/amazon-joins-tech-giants-in-backing-federal-privacy-safeguards [https://perma.cc/QTW7-ZC24].

10. *See* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 389–91 (2019) ("All U.S. companies could either comply with the GDPR or cease offering sales and services to EU consumers.").

11. *See* Ben Zimmer, *'Techlash': Whipping Up Criticism of the Top Tech Companies*, WALL STREET J. (Jan. 10, 2019), https://www.wsj.com/articles/techlash-whipping-up-criticism-of-the-top-tech-companies-11547146279 [https://perma.cc/5G42-GL2G].

12. *See* Cameron F. Kerry, *Breaking Down Proposals for Privacy Legislation: How Do They Regulate?*, BROOKINGS (Mar. 8, 2019), https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/ [https://perma.cc/6QXK-ZHSJ].

13. *See id.* (summarizing differences between proposed bills).

14. *See generally* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

15. *See* Jonas Lerman, *Big Data and Its Exclusions*, 66 STAN. L. REV. ONLINE 55 (2013), https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-and-its-exclusions/ [https://perma.cc/L3XP-FXDR]; *see also* Matthew Desmond & Bruce Western, *Poverty in America: New Directions and Debates*, 44 ANN. REV. SOC. 305, 308 (2018) (describing how social exclusion is a form of deprivation).

16. *See generally* Sarah Valentine, *Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control*, 46 FORDHAM URB. L.J. 364 (2019).

predictive policing software, which relies on data profiling to target certain neighborhoods or people.[17] These communities are also deeply concerned about facial recognition software, which is increasingly used by law enforcement and low-income housing developments.[18] The internet experience is also different for low-income people than their more affluent counterparts, both in terms of how they access the internet and the advertising that is displayed to them.[19]

These harms impede the economic security of low-income people, with ripple effects to other poverty-related deprivations, such as poor physical and mental health, family instability, threat of violence, environmental harms, low wages or lack of work, limited education, and inadequate living standards.[20] Thus, data privacy is not only integral to values such as autonomy and dignity but also an important issue of economic justice—defined here as ensuring "that everyone has access to the material resources that create opportunities, in order to live a life unencumbered by pressing economic concerns."[21]

Although this article focuses on economic justice, it is impossible to discuss class issues without recognizing how economic subordination is

---

17. *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

18. *See* Tanvi Misra, *The Tenants Fighting Back Against Facial Recognition Technology*, CITYLAB (May 7, 2019), https://www.citylab.com/equity/2019/05/facial-recognition-tech-surveillance-security-amazon-ring/588436/ [https://perma.cc/T4FB-BRSL].

19. Mary Madden, Michele E. Gilman, Karen Levy & Alice E. Marwick, *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 57 (2017); Michael Fertik, *The Rich See a Different Internet than the Poor*, SCI. AM. (Feb. 1, 2013), https://www.scientificamerican.com/article/rich-see-different-internet-than-the-poor/ [https://perma.cc/8ZUY-H6FR].

20. *See generally* BRIAN GLASSMAN, MULTIDIMENSIONAL DEPRIVATION IN THE UNITED STATES: 2017 (2019), https://www.census.gov/content/dam/Census/library/publications/2019/demo/acs-40.pdf [https://perma.cc/7JSQ-XFDM]. Among the six dimensions of poverty measured in the Multidimensional Deprivation Index, 37.1% of the United States population was deprived in one or more dimensions in 2017. *Id.* at 7. This is significantly higher than the 2017 official poverty measure based on the American Community Survey—which is based solely on income—of 13.4%. *Id.* at 2.

21. Sandro Galea, *On Economic Justice*, B.U. SCH. PUB. HEALTH (Jan. 29, 2017), https://www.bu.edu/sph/2017/01/29/on-economic-justice/ [https://perma.cc/JU48-7F2U].

Economic justice concerns include the "distribution of income, wealth, and opportunity," "individual and group rights," and "the relation of racial justice and gender justice to economic justice." Louise Simmons, *Economic Justice*, OXFORD ENCYCLOPEDIA SOC. WORK (Mar. 2017), https://oxfordre.com/socialwork/socialwork/view/10.1093/acrefore/9780199975839.001.0001/acrefore-9780199975839-e-1266 [https://perma.cc/NMA5-KYGX] (discussing various realms of economic justice).

linked to race, gender, disability, LGBTQ status, and other intersectional identities. Low socio-economic status is deeply intertwined with these attributes as a result of histories of discrimination and marginalization. At the same time, people who suffer poverty in America are a diverse and varied group of people, each with their own narratives, strengths, and challenges.[22] Still, as a group, low-income people share vulnerabilities to data privacy deprivations, which in turn pose a barrier to economic stability.[23] This article focuses on that common experience.

Given the rise of digital profiling and artificial intelligence, it is useful and timely to consider whether existing privacy laws such as the GDPR serve the needs of economically marginalized people in ways that should be incorporated into United States law. This article argues that while the GDPR is not a panacea, it contains provisions that have the potential to limit digital discrimination against the poor, while enhancing their economic stability and mobility. As a piece of legislation, the GDPR does not contain tools to dismantle oppressive structures within the economy and society that technology magnifies,[24] but it does enhance transparency and accountability, which in turn can serve social justice movements. With greater knowledge of and control over personal data flows, Americans can consider other substantive privacy interventions that might be necessary to advance economic justice, such as limitations on targeted advertising, facial recognition technology, workplace surveillance, and the like. Moreover, American corporations are already working on compliance with these statutes,[25] and in the EU, governments are busy enforcing the GDPR.[26] Thus, these provisions are within the realm of the possible and the practical. The

---

22. *See* JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 20–21 (2001) (describing demographic, political, physical, and regional variations among poor people); *see also* FRANK MUNGER, LABORING BELOW THE LINE: THE NEW ETHNOGRAPHY OF POVERTY, LOW-WAGE WORK, AND SURVIVAL IN THE GLOBAL ECONOMY 20 (Frank Munger ed., 2002) (asserting the importance of seeing and understanding the poor as individuals with their own narratives).

23. For excellent analysis of how cyberspace technologies intersect with race, see generally RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE (2019) and SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018).

24. *See* Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 FORDHAM L. REV. 613, 620 (2019) (explaining how algorithmic decision-making "represents a radical shift in the discourse of power."). Waldman adds that "algorithmic decision-making represents a distinctly neoliberal form of policy making" that enshrines values of efficiency and innovation over values "like fairness, nondiscrimination, and human rights." *Id.* at 624.

25. Rustad & Koenig, *supra* note 10, at 365.

26. *See, e.g.*, *GDPR Fines and Penalties*, NATHAN TR. (Feb. 23, 2020), https://www.nathantrust.com/gdpr-fines-penalties [https://perma.cc/5NRA-BXAF].

GDPR is providing momentum for national legislation currently being debated in Congress.[27] For political and cultural reasons, it is unlikely Congress will enact any law that is more protective of consumer interests than the GDPR. Thus, the GDPR is a viable text for thinking about how to shore up privacy for our most vulnerable communities, and it deserves extended analysis and consideration from this perspective.

Part I describes the class differential in data privacy harms, explaining how low-income people are susceptible to both unfair targeting and exclusion based on their data profiles, as well as heightened social control through surveillance. Mapping the landscape of digital privacy harms facing marginalized groups is essential to bringing their experiences into lawmaking. Part II explains why America's current data privacy legal regime, which centers on a notice and consent model, is woefully inadequate to protect the privacy of Americans, with particularly harsh consequences for low-income people. Part III analyzes five provisions in the GDPR that have the potential to advance economic justice if similar provisions are enacted at a federal level in the United States, or even in individual states.[28] These provisions are as follows: (1) the right to an explanation about automated decision-making; (2) the right not to be subject to decisions based on solely automated profiling; (3) the right to be forgotten; (4) public participation in data processing programs; and (5) robust implementation and enforcement tools. Part IV considers how the California Consumer Privacy Act compares to the GDPR in terms of economic justice objectives. While data privacy has been aptly recognized as a civil rights issue,[29] this article contends that data

---

27. *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 773 (2019) ("The EU has taken an essential role in shaping how the world thinks about data privacy."); *see also* CONG. RESEARCH SERV., DATA PROTECTION LAW: AN OVERVIEW 50–51 (2019) https://fas.org/sgp/crs/misc/R45631.pdf [https://perma.cc/84W6-VTQX]; *cf.* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, MINN. L. REV. (forthcoming 2020), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3208&context=facpub [https://perma.cc/VM7V-UXLH] (arguing that the California law is catalyzing privacy law across the United States).

28. Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1063 (2019) (noting that some states "have already begun to emulate certain aspects of the GDPR").

29. *See* Letter from Access Humbolt et al., to Sen. Roger Wicker et al., (Feb. 13, 2019), https://www.democraticmedia.org/sites/default/files/field/public-files/2019/letter_to_congress_on_civil_rights_and_privacy_2-13-19.pdf [https://perma.cc/7HSN-FBUY] (writing "to ensure that civil rights retain a fundamental place in the ongoing privacy debate"); Becky Chao, Eric Null & Brandi Collins-Dexter, *Centering Civil Rights in the Privacy Debate*, NEW AM. (Aug. 14, 2019), https://www.newamerica.org/oti/reports/centering-civil-rights-privacy-debate/ [https://perma.cc/W52Z-TJ2C]; Aaron Rieke & Corrine Yu, *Discrimination's Digital Frontier*,

privacy is also an economic justice issue, and that both frames are essential for enacting laws that benefit marginalized communities. The GDPR contains mechanisms to combat illegal discrimination as well as to move towards a substantive vision of economic justice.

II. THE CLASS DIFFERENTIAL IN DATA PRIVACY HARMS

At all hours of the day, and deep into the night, our data is being harvested, aggregated, and sold.[30] Businesses generate immense profits from this mining of big data, making use of our buying habits, social relationships, political preferences, lifestyle, hobbies, health, and personality.[31] The data extraction industry relies on a wide range of sources, such as public records, web browsing activity, emails, banking activity, social media, store loyalty cards, online quizzes, license plate readers, app usage, smart devices (such as fitness watches and internet-connected doorbells), and geo-location tracking on our smartphones.[32] "Increasingly, the market sees you from within, measuring your body and emotional states, and watching as you move around your house, the office, or the mall."[33] Data brokers combine and cross-reference the "different sources of information they've bought and acquired, and then create a single detailed file on you: a data profile of your digital shadow."[34] Data brokers sell these profiles to eager purchasers, including marketers and

---

ATLANTIC (Apr. 15, 2019), https://www.theatlantic.com/ideas/archive/2019/04/facebook-targeted-marketing-perpetuates-discrimination/587059/ [https://perma.cc/7HJR-FW4U].

30. *See* IGO, *supra* note 2, at 355; Geoffrey A. Fowler, *It's the Middle of the Night. Do You Know Who Your iPhone Is Talking to?*, WASH. POST (May 28, 2019), https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/ [https://perma.cc/BZ83-VZLV].

31. *See* Wolfie Christl, *Corporate Surveillance in Everyday Life*, CRACKED LABS (June 2017), https://crackedlabs.org/en/corporate-surveillance/ [https://perma.cc/JEY5-LWHV]; Jeremy B. Merrill, *How to Wrestle Your Data From Data Brokers, Silicon Valley—and Cambridge Analytica*, PROPUBLICA (Apr. 30, 2018), https://www.propublica.org/article/how-to-wrestle-your-data-from-data-brokers-silicon-valley-and-cambridge-analytica [https://perma.cc/FK3J-RK7X].

32. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/BY66-56VQ]; Stuart A. Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/5YDZ-WU6G] (reporting on the ease of matching billions of location data points originating from a single data location company with specific individuals).

33. Marion Fourcade & Kieran Healy, *Seeing Like a Market*, 15 SOCIO-ECON. REV. 9, 23 (2017).

34. HANNAH FRY, HELLO WORLD, BEING HUMAN IN THE AGE OF ALGORITHMS 32 (2018).

retailers, law enforcement, financial companies, educational institutions, employers, and government agencies, who then use the data for their own purposes.[35] Big Tech companies such as Amazon, Google, and Facebook are also mining their consumers' data and selling access to this information trove to advertisers.[36] In addition, almost every major industry is using their customer's data to integrate with these data networks in order to expand their profits.[37] Government agencies both sell and purchase their citizens' personal data, thus blurring the distinction between public and private harms and remedies.

There is a longstanding tension between Americans' desire for privacy and the "free" services provided by social media and search engines.[38] A Pew survey on social media usage found that ninety-one percent of Americans are concerned about lacking control over their personal information.[39] And yet, only one in ten Facebook users exited the platform after learning about the Cambridge Analytica scandal.[40] For many people, it appears that the harms of the surveillance economy do not rise beyond a sense of creepiness at being followed around the web by ads for products they briefly perused online. This apathy is slowly changing, however, as Americans learn more about the consequences of their data collection. For instance, while most Americans remain on Facebook, many are changing their online behavior, some are

35. *Id.* at 31; FED. TRADE COMM'N, *supra* note 32.

36. *See* FRY, *supra* note 34, at 36; Steve Lohr, *Calls Mount To Ease Big Tech's Grip on Your Data*, N.Y. TIMES (July 25, 2019), https://www.nytimes.com/2019/07/25/business/calls-mount-to-ease-big-techs-grip-on-your-data.html [https://perma.cc/V4L8-SEN6]; Angela Moscaritolo, *What Does Big Tech Know About You? Basically Everything*, PC MAG (Apr. 8, 2020), https://www.pcmag.com/news/366327/what-does-big-tech-know-about-you-basically-everything [https://perma.cc/U5ND-6X2S]; *The Rise of Data Capital*, MIT TECH. REV. CUSTOM & ORACLE (2016), http://files.technologyreview.com/whitepapers/MIT_Oracle+Report-The_Rise_of_Data_Capital.pdf [https://perma.cc/2XDG-URQY].

37. *See* Christl, *supra* note 31.

38. Max Eddy, *Online Data Protection 101: Don't Let Big Tech Get Rich Off Your Info*, PC MAG (Oct. 10, 2018), https://www.pcmag.com/news/online-data-protection-101-dont-let-big-tech-get-rich-off-your-info [https://perma.cc/2CBC-MAZE].

39. *See* Rainie, *supra* note 5.

40. Chris Raymond, *So What Do You Think of Facebook Now?*, CONSUMER REP. (Mar. 15, 2019), https://www.consumerreports.org/social-media/what-do-you-think-of-facebook-now-survey/ [https://perma.cc/4PT3-4CVW]. Even when people exit Facebook—or never engage with it in the first place—it maintains "shadow profiles" on them. *See* Russell Brandom, *Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense*, VERGE (Apr. 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy [https://perma.cc/Q3T8-7F27]; Sarah Jeong, *I Tried Leaving Facebook. I Couldn't*, VERGE (Apr. 28, 2018), https://www.theverge.com/2018/4/28/17293056/facebook-deletefacebook-social-network-monopoly [https://perma.cc/HA2G-686G].

actively subverting surveillance technologies,[41] and large majorities believe we need stronger legal protections for our data.[42]

The need for greater legal protections is particularly acute for low-income people,[43] who pay the highest price for our surveillance economy. We live in "a data environment . . . in which individuals are constantly surveyed and evaluated, categorized and grouped, rated and ranked, numbered and quantified, included or excluded, and as a result, treated differently."[44] In one sense, this is nothing new—poor people have been stigmatized and surveilled for centuries.[45] However, technology is hyper-charging this dynamic, while simultaneously obscuring the structural disadvantages that oppress low-income populations.[46] The big data ecosystem and its algorithmic outputs, along with a corresponding lack of privacy protections, undermine economic justice for marginalized people in at least three overarching and intersecting ways, subjecting them to digital discrimination and electronic exploitation; inaccuracies; and surveillance.[47]

---

41. *See, e.g.*, Elise Thomas, *How To Hack Your Face To Dodge the Rise of Facial Recognition Tech*, WIRED (Feb. 1, 2019), https://www.wired.co.uk/article/avoid-facial-recognition-software [https://perma.cc/VP6N-9R78]; Malia Wollan, *How To Thwart Facial Recognition*, N.Y. TIMES (July 30, 2019), https://www.nytimes.com/2019/07/30/magazine/how-to-thwart-facial-recognition.html [https://perma.cc/GSS7-WG9A].

42. *See* Raine, *supra* note 5.

43. This article defines the words "low-income" and "poverty" and "low socio-economic status" to mean people living under "economic deprivation"—or lack of economic resources with attendant negative social consequences—without endorsing any particular method of measuring poverty. *See* JOHN ICELAND, POVERTY IN AMERICA: A HANDBOOK 23 (3d ed. 2013) (defining poverty). The United States uses an absolute measure in calculating the official poverty line (i.e., it is based on a needs standard that is constant over time), whereas relative measures are based on comparative disadvantage, fluctuating over time. *Id.* at 23–24. Under federal government measures, the poverty line is generally a lower financial threshold than the standards used to define low-income. *See* Alicia Mazzara & Barbara Sard, *Chart Book: Employment and Earnings for Households Receiving Federal Rental Assistance*, CTR. ON BUDGET & POL'Y PRIORITIES (Feb. 5, 2018), https://www.cbpp.org/research/housing/chart-book-employment-and-earnings-for-households-receiving-federal-rental#_ftn5 [https://perma.cc/9XYL-JWLC]. On the various methods of measuring poverty and their controversies and merits, see generally ICELAND, *supra* at ch. 3.

44. *See* Christl, *supra* note 31.

45. *See* VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 14–38 (2018); Wendy A. Bach, *Prosecuting Poverty, Criminalizing Care*, 60 WM. & MARY L. REV. 809, 818–20 (2019).

46. EUBANKS, *supra* note 45, at 33–37; IGO, *supra* note 2, at 357 ("What gives the current moment its special urgency is a uniquely combustible combination: a deluge of volunteered or solicited personal information, on the one hand, and the increasingly sophisticated capacities of other parties for linking, sharing, and acting on it, on the other.").

47. There are numerous, serious other big data harms and technological privacy intrusions outside the scope of this article, such as immigration surveillance, online targeting of women in

A. Digital Discrimination/Electronic Exploitation

People with low socio-economic status face both digital discrimination and economic exploitation when businesses and government use technological tools to target them for unfair products and services or to exclude them from mainstream opportunities. These tools add scope, scale, and speed to long-standing economic vulnerabilities. Algorithmic decision-making,[48] or computerized analysis of large data sets to infer correlations, is fueling these patterns of targeting and exclusion, thus making it harder for low-income people to move up the economic ladder.[49] Employers use algorithms to decide who to target with job postings, who to interview, and who to hire.[50] Landlords use tenant screening reports generated by algorithms to assess who is likely to pay their rent on time.[51] Colleges use algorithms to identify applicants who are most likely to attend and to stay in school.[52] Government social service agencies use algorithms to determine program eligibility and track recipients' compliance.[53] Law enforcement agencies use algorithms to predict criminal hot spots and identify suspects.[54] The criminal justice system uses algorithms to determine bail on the front end and sentencing on the back end.[55] While these examples can all encompass legitimate societal objectives, inequities arise when algorithms reinforce

---

ways that threaten their personal safety, and online disinformation campaigns. In addition, poor people suffer greater injuries resulting from data breaches, and thus benefit from enhanced cybersecurity efforts and enforcement. *See* Sarah Dranoff, *Identity Theft: A Low-Income Issue*, A.B.A. (Dec. 15, 2014), https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/ [https://perma.cc/2PNX-FYVM].

48. Some algorithms are rule-based, meaning they are human constructed and "direct and unambiguous," such as an automated decision tree. FRY, *supra* note 34, at 10. Other algorithms are used in machine learning (a form of artificial intelligence or AI), which "refers to an automated process of discovering correlations . . . between variables in a dataset, often to make predictions or estimates of some outcome." David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 671 (2017).

49. Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1026–27 (2017) (examples of discrimination); *Id.* at 1036–39 (means by which discrimination operates unintentionally in algorithms).

50. *See* Stephanie Bornstein, *Antidiscriminatory Algorithms*, 70 ALA. L. REV. 519, 530–33 (2018).

51. James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 FORDHAM URB. L.J. 219, 251–53 (2019).

52. Madden et al., *supra* note 19, at 98–103.

53. Valentine, *supra* note 16, at 370–71.

54. FRY, *supra* note 34, at 154–59; Emily Berman, *A Government of Laws and Not of Machines*, 98 B.U. L. REV. 1277, 1293 (2018); Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043, 1049–50, 1068–72 (2019).

55. Huq, *supra* note 54, at 1072–76.

divides in economic status or result in discrimination against marginalized groups.

Employment. There are numerous examples of algorithms that discriminated against people who are protected under anti-discrimination civil rights laws.[56] For instance, Amazon tested a hiring algorithm for technical jobs that turned out to be biased against women.[57] The programmers fed data into the algorithm culled from Amazon's prior ten years of resumes, which were predominated by white males. The algorithm then linked the traits on those resumes to predictions about future success, thereby disfavoring resumes that contained words associated with women.[58] Similarly, a study that tested Google's ad platform created a simulation that found that ads related to career coaching for high paid executive positions were funneled more frequently to men than women, although the cause was unclear.[59] It "might have resulted unintentionally from algorithms optimizing click-through rates or other metrics free of bigotry."[60]

In legal terms, this may have been a case of disparate impact, or the differential treatment of certain groups based on neutral criteria.[61] In practical terms, it means that women may continue to suffer from a gender pay gap that leaves them disproportionately underpaid compared to men, which

---

56. Federal laws prohibit discrimination on the on the basis of race, color, national origin, religion, age, gender, pregnancy, veteran's status, genetic information, and physical or mental disability. *See, e.g.*, 42 U.S.C. § 2000e (2018). Some state laws protect additional groups. *See EEO Protected Classes by State and Municipality*, XPERTHR, https://www.xperthr.com/fifty-state-charts/eeo-protected-classes-by-state-and-municipality/9953/ [https://perma.cc/P6NN-NW2Y].

57. Nicol Turner Lee, Paul Resnick & Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies To Reduce Consumer Harms*, BROOKINGS (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/#footref-10 [https://perma.cc/XY6N-HGGL].

58. *Id.* Amazon is 60% male and 74% of managers are male. *Id.* The company says it did not implement the hiring tool. *Id.*; *see also* Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 9, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/9T7Y-L7CL].

59. Amit Datta, Michael Carl Tschantz & Anupam Datta, *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*, 1 PROC. ON PRIVACY ENHANCING TECHS. 92 (2015), http://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf [https://perma.cc/Q4AU-6B2E].

60. *Id.* at 105.

61. On the difference between disparate impact and disparate treatment theories in discrimination law, see Deborah L. Brake, *The Shifting Sands of Employment Discrimination: From Unjustified Impact to Disparate Treatment in Pregnancy and Pay*, 105 GEO. L.J 559, 564–69 (2017).

contributes to the feminization of poverty, or higher rates of poverty among women.[62] Another example comes from a hiring algorithm designed to predict employee tenure; it found the single best predictor of tenure was distance between home and work,[63] a factor that was highly correlated with race.[64] In turn, racial discrimination in employment compounds the racial wealth gap and perpetuates disproportionate poverty for African-Americans.[65] "Since many social patterns related to education and work reflect troubled legacies of racism, sexism, and other forms of socioeconomic disadvantage, blindly replicating those patterns via software will only perpetuate and exacerbate historical disparities."[66]

In 2019, Facebook settled five lawsuits brought by civil rights organizations and individuals alleging that it permitted housing, job, and loan companies to micro-target advertisements on Facebook's platform to certain groups.[67] Among the alleged wrongdoing, Facebook's ad system excluded

---

62. *See* ICELAND, *supra* note 43, at 99–100; Michele E. Gilman, *En-Gendering Economic Inequality*, 32 COLUM. J. GENDER & L. 1, 9–13 (2016).

63. Joseph Walker, *Meet the New Boss: Big Data*, WALL STREET J. (Sept. 20, 2012), https://www.wsj.com/articles/SB10000872396390443890304578006252019616768 [https://perma.cc/SM69-6YD8]. The company dropped that variable. *Id.*

64. *Id.*

65. *See* Brentin Mock, *Why Can't We Close the Racial Wealth Gap?*, CITYLAB (Mar. 21, 2019), https://www.citylab.com/equity/2019/03/racial-wealth-gap-income-inequality-black-white-households/585325/ [https://perma.cc/35V6-SPFC] (reporting on a study of how the racial income gap feeds the racial wealth gap); Thomas Shapiro, Tatjana Meschede & Sam Osoro, *The Roots of the Widening Racial Wealth Gap: Explaining the Black-White Economic Divide*, INST. ON ASSETS & SOC. POL'Y (2013), https://heller.brandeis.edu/iasp/pdfs/racial-wealth-equity/racial-wealth-gap/roots-widening-racial-wealth-gap.pdf [https://perma.cc/TG2Z-AQUF].

66. MIRANDA BOGEN & AARON RIEKE, HELP WANTED: AN EXAMINATION OF HIRING ALGORITHMS, EQUITY, AND BIAS 8 (Dec. 2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf [https://perma.cc/W24P-2QXE].

67. Tracy Jan & Elizabeth Dwoskin, *Facebook Agrees To Overhaul Targeted Advertising System for Job, Housing and Loan Ads After Discrimination Complaints*, WASH. POST (Mar. 19, 2019), https://www.washingtonpost.com/business/economy/facebook-agrees-to-dismantle-targeted-advertising-system-for-job-housing-and-loan-ads-after-discrimination-complaints/2019/03/19/7dc9b5fa-4983-11e9-b79a-961983b7e0cd_story.html [https://perma.cc/G2X7-V536]. ProPublica reporting uncovered the micro-targeting. Julia Angwin & Terry Parris, Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA (Oct. 28, 2016), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race [https://perma.cc/R8XD-WY58]; Julia Angwin, Ariana Tobin & Madeleine Varner, *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/KF62-8WVL]; Julia Angwin, Noam Scheiber & Ariana Tobin, *Dozens of Companies Are Using Facebook To Exclude Older Workers from Job Ads*,

people with a certain "ethnic affinity" from seeing housing ads[68] and excluded women from viewing job postings that employers wanted targeted to men, such as Uber drivers, truck drivers, and roofers.[69] To offer this targeted advertising, Facebook classified people into more than 50,000 categories such as "English as a second language," "disabled parking permit," or "Telemundo."[70]

Under the terms of the settlement,[71] Facebook's advertisers will no longer be able to target people based on sensitive categories such as age, gender, zip code, or race. However, a study found that advertising discrimination on Facebook persists post-settlement apparently because the modified algorithms target viewers based on proxy variables and ad content.[72] Moreover, targeting by income is not prohibited under the settlement,[73] just as poverty is not a protected class under discrimination law.[74] This legal gap magnifies economic inequality. People click on certain ads, while skipping others, due to "deep-seated social inequities: the neighborhood they live in, where they went to school, how much money they have. An ad system that is designed to maximize clicks, and to maximize profits for Facebook, will naturally reinforce these social inequities and so serve as a barrier to equal opportunity."[75]

PROPUBLICA (Dec. 20, 2017), https://www.propublica.org/article/facebook-ads-age-discrimination-targeting [https://perma.cc/FE9A-9QRV].

68. *See* Jan & Dwoskin, *supra* note 67.

69. *See* Nitasha Tiku, *ACLU Says Facebook Ads Let Employers Favor Men over Women*, WIRED (Sept. 18, 2018), https://www.wired.com/story/aclu-says-facebook-ads-let-employers-favor-men-over-women/ [https://perma.cc/WM35-KEBZ].

70. *See* Jan & Dwoskin, *supra* note 67. Facebook is facing a separate class action lawsuit alleging age and gender discrimination in the financial advertising it serves on its platform. *See* John Detrixhe & Jeremy B. Merrill, *The Fight Against Financial Advertisers Using Facebook for Digital Redlining*, QUARTZ (Nov. 1, 2019), https://qz.com/1733345/the-fight-against-discriminatory-financial-ads-on-facebook/ [https://perma.cc/A69L-VSS2].

71. For the settlement agreement of claims brought by housing advocates, see *Settlement Agreement and Release Between National Fair Housing Alliance et al., and Facebook*, NAT'L FAIR HOUSING ALLIANCE (Mar. 28, 2019), https://nationalfairhousing.org/wp-content/uploads/2019/03/FINAL-SIGNED-NFHA-FB-Settlement-Agreement-00368652x9CCC2.pdf [https://perma.cc/K7G7-V2FJ] [hereinafter *Settlement Agreement*].

72. Piotr Sapiezynski et al., *Algorithms that "Don't See Color": Comparing Biases in Lookalike and Special Ad Audiences* (2019), https://arxiv.org/pdf/1912.07579.pdf [https://perma.cc/3L7C-8RLT].

73. Targeting by source of lawful income is prohibited under the settlement. *Settlement Agreement*, *supra* note 71.

74. Danieli Evans Peterman, *Socioeconomic Status Discrimination*, 104 VA. L. REV. 1283, 1291–92, 1300 (2018).

75. Rieke & Yu, *supra* note 29.

Education. Big data is used not only to discriminate among groups but also to exploit marginalized groups. Poverty has many causes; it "is not simply the byproduct of one's attributes or historical outcomes but is also actively produced through unequal relationships between the financially secure and insecure."[76] An exploitative relationship is exemplified in the for-profit higher educational field, where "lead generation" websites surreptitiously gather information about potential students when people conduct web searches for terms such as welfare benefits.[77] The lead generators target low-income people and veterans and then sell their personal data to for-profit colleges, who subsequently apply deceptive and strong-armed marketing tactics to potential students, encouraging them to take out massive loans to enroll.[78] At these for-profit colleges, students often assume crippling debt with few job prospects and low graduation rates.[79]

Within the non-profit college landscape, some colleges use tracking software to collect and analyze data on high school students who visit their admissions websites (without the students' knowledge).[80] Algorithms then identify which students are most likely to attend and pay full tuition rates.[81] When admission offices use these algorithms to focus on affluent students, underprivileged high school students may end up excluded from recruiting efforts. Algorithms provide increased opportunities for economic segmentation.

Financial Services. Another example of data exploitation arises in the financial services setting. Online lead generation is steering low-income, predominantly African-American consumers to high-interest payday loans.[82] These ads are able to reach consumers even in states where payday lending

---

76. Desmond & Western, *supra* note 15, at 310.

77. *See* U.S. PUB. INTEREST RESEARCH GRP. & CTR. FOR DIG. DEMOCRACY, PRIVATE FOR-PROFIT COLLEGES AND ONLINE LEAD GENERATION: PRIVATE UNIVERSITIES USE DIGITAL MARKETING TO TARGET PROSPECTS, INCLUDING VETERANS, VIA THE INTERNET (May 2015), https://www.democraticmedia.org/sites/default/files/field/public-files/2015/forprofitcollegeleadgenreport_may2015_uspirgef_cdd_0.pdf [https://perma.cc/KVD6-T773].

78. *Id.*

79. *See* Maura Dundon, *Students or Consumers? For-Profit Colleges and the Practical and Theoretical Role of Consumer Protection*, 9 HARV. L. & POL'Y REV. 375, 376–77 (2015).

80. Douglas MacMillan & Nick Anderson, *Student Tracking, Secret Scores: How College Admissions Offices Rank Prospects Before They Apply*, WASH. POST (Oct. 14, 2019), https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/ [https://perma.cc/YTV8-SYL4].

81. *Id.*

82. UPTURN, LED ASTRAY: ONLINE LEAD GENERATION AND PAYDAY LOANS (Oct. 2015), https://www.upturn.org/static/reports/2015/led-astray/files/Upturn_-_Led_Astray_v.1.01.pdf [https://perma.cc/Z8MD-87WJ].

is unlawful.[83] One lead generator provides payday loan companies with highly segmented lists that identify "consumers who are struggling to make their bills and are looking for fast quick cash."[84] Payday loans are financially harmful because they charge high interest rates that are difficult for low-income borrowers to pay back, thus placing them in an endless loop of high-interest borrowing to cover existing loans.[85] Moreover, the industry is rife with lax data security.[86] The market in consumer data propels this consumer exploitation.

In the mainstream financial market, credit scores are used to determine the costs of borrowing money, and they are incorporated into reports used by the gatekeepers to housing, employment, professional licensing, and education.[87] Thus, a low score can depress economic mobility,[88] and certain groups within society predictably have lower scores. "A good credit score is usually a proxy for wealth, and wealth is a good proxy for race and national origin."[89] Further, many minorities are "credit invisible"—due to generations of discrimination by banks, they have avoided mainstream financial services altogether and thus do not generate the sort of information that feeds a credit score.[90] Members of this "lumpenscoretariat" have economic lives outside the formal economy.[91]

Given these dynamics, there are concerns that mainstream credit scoring models exclude alternate data points that could assist minorities in obtaining

---

83. *Id.*; *Comments of Alvaro Bedoya and Clare Garvie, Center on Privacy & Technology at Georgetown Law, on "Follow the Lead: An FTC Workshop on Lead Generation*," FED. TRADE COMMISSION (Dec. 18, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/12/00017-99877.pdf [https://perma.cc/Q8YU-4SHM] [hereinafter *Bedoya & Garvie*].

84. *Bedoya & Garvie*, *supra* note 83.

85. *See* UPTURN, *supra* note 82.

86. *Id.*

87. *See* Vlad A. Hertza, *Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?*, 93 N.Y.U. L. REV. 1707, 1713 (2018); Lea Shepard, *Toward a Stronger Financial History Antidiscrimination Norm*, 53 B.C. L. REV. 1695, 1696 (2012).

88. Shepard, *supra* note 87, at 1734.

89. Hertza, *supra* note 87, at 1727.

90. *See* Lori T. Yearwood, *Many Minorities Avoid Seeking Credit due to Generations of Discrimination. Why That Keeps Them Back*, CNBC (Sept. 1, 2019), https://www.cnbc.com/2019/09/01/many-minorities-avoid-seeking-credit-due-to-decades-of-discrimination.html [https://perma.cc/6YHZ-EFDX] ("Decades of discrimination by the federal government and America's financial institutions has induced an almost trauma-like response, causing many people of color, particularly African-Americans, to adopt self-protective behavior not unlike a post-traumatic stress reaction.").

91. Fourcade & Healy, *supra* note 33, at 19. In the cloud economy, "Those who are invisible are of little use." *Id.*

better credit terms, such as utility and rental payments, while instead relying upon traditional data points that magnify existing disparities in access to "high-quality education, well-paying jobs, and affordable loans."[92] At the same time, there is caution that alternative data points might "be designed to identify and target vulnerable individuals with high-cost loan products."[93] Without careful design and oversight, both traditional and alternative credit rating models raise the risk that affordable credit will remain out of reach for low-income consumers.

Housing. Automated decision-making by lenders is associated with higher mortgage rates for Black and Latino borrowers as compared to similarly situated white borrowers.[94] Although the disparity is lower for fintech mortgages than for traditional mortgages, this finding contradicts claims that algorithms eliminate discrimination.[95] All told, Black and Latino borrowers are paying up to three quarters of a billion dollars more in mortgage interest each year.[96] Given the links between wealth accumulation and homeownership, this mortgage disparity further drives the racial wealth gap.[97]

In the rental market, many landlords are screening tenants with algorithmically generated reports purchased from tenant screening companies. A fair housing lawsuit is pending in Connecticut against a tenant

---

92. *See* Shepard, *supra* note 87, at 1731.

93. Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 YALE J.L. & TECH. 148, 167 (2017).

94. Aaron Glantz & Emmanuel Martinez, *Kept Out: For People of Color, Banks Are Shutting the Door to Homeownership*, REVEAL (Feb. 15, 2018), https://www.revealnews.org/article/for-people-of-color-banks-are-shutting-the-door-to-homeownership/ [https://perma.cc/555W-6E78].

95. Emily Badger, *Who's To Blame When Algorithms Discriminate?*, N.Y. TIMES (Aug. 22, 2019), https://www.nytimes.com/2019/08/20/upshot/housing-discrimination-algorithms-hud.html [https://perma.cc/6HWR-YDKV] (describing the research of law professor Myron Orfield, who states that "[a] black household that makes $167,000 is less likely to qualify for a prime loan [for a mortgage] than a white household that makes $40,000"); Robert Bartlett et al., Consumer-Lending Discrimination in the FinTech Era 6 (Nov. 2019) (unpublished manuscript), http://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf?_ga=2.106485891.1035370151.1559599414-527767480.1559599414 [https://perma.cc/X7YN-VHXC]; Glantz & Martinez, *supra* note 94 (reporting that an analysis of thirty-one million records showed minorities were charged mortgage loans at higher rates than their white counterparts in sixty-one metro areas "even when controlling for applicants' income, loan amount and neighborhood").

96. Bartlett et al., *supra* note 95, at 5. The study found that the fintech lenders discriminated less than face-to-face lenders in terms of accepting minority applications. *Id.* at 6. This is a good example of automated decision overcoming human biases.

97. Glantz & Martinez, *supra* note 94. HUD is proposing new regulations that would limit the ability to challenge algorithmic screening used by landlords. *See* Badger, *supra* note 95.

screening company that incorporates criminal record data in its reports.[98] The plaintiffs allege that this practice reflects and compounds the effects of high levels of policing in minority neighborhoods.[99] Indeed, screening tools that include criminal record data disproportionately impact African Americans and Hispanics (even though whites engage in similar rates of criminal behavior), and reliance on these reports can leave people homeless or reduced to living in substandard housing.[100] The problem is compounded when, as in the Connecticut case, the creator of the algorithm refuses to reveal information about the source or details of the underlying criminal history records, making it impossible for a landlord to consider—or a tenant to challenge—whether the supposed criminal conduct at issue should be disqualifying.[101]

Health Care. Health care analytics based on personal data can help guide patient diagnosis and treatment, but they can also lead to digital discrimination.[102] The Health Insurance Portability and Accountability Act, or HIPAA, aims to protect patient privacy by preventing health care providers from unauthorized use or disclosure of patients' medical data.[103] However, HIPAA permits health care providers to share patient data with business associates, and this means that Google can partner with Ascension, a health care chain operating in twenty-one states, in order to collect and analyze the health data of millions of Ascension patients without the knowledge or consent of the patients or their doctors.[104] This partnership is raising concerns

---

98. Mark Pazniokas, *A Tenant Blacklist, Compiled by Algorithm*, CONN. MIRROR (Mar. 28, 2019), https://ctmirror.org/2019/03/28/a-tenant-blacklist-compiled-by-algorithm/ [https://perma.cc/CJ58-H43U].

99. *See id.*

100. *See Arroyo v. Corelogic*, NAT'L HOUSING L. PROJECT (July 31, 2018), https://www.nhlp.org/our-initiatives/arroyo-v-corelogic/ [https://perma.cc/ZF79-B37T].

101. *See* Pazniokas, *supra* note 98.

102. *See generally* Alvin Rajkomar et al., *Ensuring Fairness in Machine Learning To Advance Health Equity*, 169 ANNALS INTERNAL MED. 866 (2018); Linda Nordling, *A Fairer Way Forward for AI in Health Care*, NATURE (Sept. 25, 2019), https://www.nature.com/articles/d41586-019-02872-2 [https://perma.cc/9MXP-RWNT]; Mohana Ravindranath, *How Your Health Information Is Sold and Turned into 'Risk Scores*,*'* POLITICO (Feb. 3, 2019), https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978 [https://perma.cc/CW4U-J6AG].

103. Sharona Hoffman, *What Genetic Testing Teaches About Predictive Health Analytics Regulation*, 98 N.C. L. REV. 123, 144 (2019).

104. Rob Copeland, *Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans*, WALL STREET J. (Nov. 11, 2019), https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790 [https://perma.cc/BQ2S-7MZZ].

about the security of patient data in light of prior data leaks at Google, as well as how the data will be used, and possibly monetized.[105]

HIPAA's scope is also limited because much health care data exists outside the scope of covered entities, such as data generated from website searches, social media platforms, app usage, and fitness trackers.[106] There are data brokers that gather this information and then sell "sick lists" to companies that in turn use the information to market products to consumers.[107] For instance, one list of 4.7 million people is called "suffering seniors," and it includes people over fifty-five who supposedly suffer from illnesses such as Alzheimer's disease and depression.[108] Data brokers also sell health profiles to insurers, who can then combine these profiles with electronic medical records and other data sets to make predictions about patient health.[109] In one cautionary tale, a woman was denied insurance because her prescription history revealed she was taking antidepressants.[110] There are companies that are generating risk scores based on health data and selling those scores to doctors, insurers, and hospitals.[111] The market in predictive health data is particularly pernicious for poor people, who have higher rates of illnesses than the general population, and may thus face higher insurance and borrowing rates, along with greater employer unwillingness to

105. Katherine Bindley, *Your Health Data Isn't as Safe as You Think*, WALL STREET J. (Nov. 22, 2019), https://www.wsj.com/articles/your-health-data-isnt-as-safe-as-you-think-11574418606 [https://perma.cc/B9RQ-ER76].

106. *See* Hoffman, *supra* note 103, at 135; Frank Pasquale & Tara A. Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 637 (2014) ("So many online activities have some implications about a person's health status that access to medical records is not necessary to construct a medical reputation."); Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385, 405–06 (2012).

107. Aimee Picchi, *The Creepy Side of Data Mining: Selling "Sick" Lists*, CBS NEWS (Sept. 11, 2014), https://www.cbsnews.com/news/the-creepy-side-of-data-mining-selling-sick-lists/ [https://perma.cc/PGD6-AWD5].

108. *Id.*

109. Max N. Helveston, *Reining in Commercial Exploitation of Consumer Data*, 123 PENN ST. L. REV. 667, 673 (2019) ("[T]he aggregation of massive amounts of consumers' personal data and advancements in AI-driven algorithmic learning have made it possible to derive almost limitless correlations between individual characteristics and risk."); Sharona Hoffman, *Big Data and the Americans with Disabilities Act*, 68 HASTINGS L.J. 777, 780–84 (2017); Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, PROPUBLICA (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/75W9-HTA8].

110. Pasquale & Ragone, *supra* note 106, at 634. Julie Brill, a former FTC Commissioner, revealed that one data broker "reportedly sells the names, mailing addresses, and medication lists of people with diseases like cancer or clinical depression. Another data broker . . . reportedly offers lists of consumers, their credit scores, and their specific ailments" to marketers. *Id.* at 630.

111. *See* Ravindranath, *supra* note 102.

hire them, as these businesses seek to cherry pick the healthiest people to reduce their future costs.[112]

Criminal Justice. The criminal justice system is also turning to algorithms, particularly in the realms of predictive policing, bail determinations, and sentencing.[113] The goal is to replace flawed human decision-making with objective, scientific rigor, but the evidence shows that human biases remain in computerized systems. These algorithms can compound the mass incarceration of minorities, which among its many harms, depletes their economic stability and reinforces poverty.[114] Police departments across the country are using predictive policing software to identify crime hot spots as well as likely offenders.[115] Criminal justice critics charge that the software is merely sending police back to locations with high numbers of arrests, thereby creating a "self-reinforcing feedback loop"[116] that "perpetuate[s] historical biases in enforcement."[117]

Algorithms are also used to conduct risk assessments that aim to determine a defendant's dangerousness; judges then use these scores in setting bail and determining criminal sentences.[118] Here too, an algorithm fed on historical crime data will reinforce discriminatory patterns of law enforcement.[119] As

---

112. Hoffman, *supra* note 103, at 139–40; Allen, *supra* note 109. Hoffman notes that the Americans with Disabilities Act does not apply to discriminatory predictions about future health problems; it applies only to discrimination based on current health conditions. Hoffman, *supra* note 103, at 150.

113. Sandra G. Mayson, *Bias in, Bias out*, 128 YALE L.J. 2218, 2227–32 (2019).

114. *See generally* MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS (2010).

115. *See* FERGUSON, *supra* note 17; Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 113–14 (2017). Selbst discusses both place-based and people-based predictive policing tools. *Id.* at 129–40.

116. Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm Is Fundamentally Flawed*, VICE (Feb. 14, 2019), https://www.vice.com/en_us/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed [https://perma.cc/F2KU-P53Z].

117. William Isaac & Kristian Lum, *Setting the Record Straight on Predictive Policing and Race*, APPEAL (Jan. 3, 2018), https://theappeal.org/setting-the-record-straight-on-predictive-policing-and-race-fe588b457ca2/ [https://perma.cc/QTT4-Q9JB]; *see also* Kristian Lum & William Isaac, *To Predict and Serve?*, 13 SIGNIFICANCE 14, 18 (2016); Mayson, *supra* note 113, at 2253 ("The choice to predict arrest has profound consequences for racial equity because in most places, for nearly all crime categories, arrest rates have been racially disparate for decades."); Selbst, *supra* note 115, at 121; Dorothy E. Roberts, *Digitizing the Carceral State*, 132 HARV. L. REV. 1695, 1720 (2019) (book review).

118. Karen Hao, *AI Is Sending People to Jail—and Getting It Wrong*, MIT TECH. REV. (Jan. 21, 2019), https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai [https://perma.cc/8KHY-DDCV].

119. *See id.*

Dorothy Roberts states, "Computerized risk assessments are based on data taken from a social context that has already been shaped by hierarchies of race, class, and gender."[120] A *ProPublica* investigative report found that a risk assessment tool called COMPAS was predicting that black defendants pose a higher risk of recidivism than they do (false positives), while under-predicting the risk for white defendants (false negatives).[121] A subsequent study concluded that the algorithm was no better at predicting risk than random people solicited for an internet survey.[122]

COMPAS and similar recidivism prediction algorithms claim not to include race as a factor, but they do include factors related to socioeconomic status, such as public benefits receipt and high school grades.[123] The inclusion of these data points "involves the state explicitly telling judges that poor people should get longer sentences because they are poor—and, conversely, that socioeconomic privilege should translate into leniency."[124] Moreover, these predictive algorithms lack transparency, and attempts to access their underlying source code or model inevitably bump up against their makers' claims that the algorithm is a protected trade secret, thus depriving defendants of due process and any ability to counter the determinations.[125] This masks the normative and policy choices embedded in algorithms.[126] On top of this, algorithmic discrimination is further compounded by "automation bias": the psychological phenomenon in which human decision-makers overly defer to computerized outputs due to their veneer of objectivity.[127] If judges do not understand how algorithms work and their potential biases and errors, they are likely to accede to computerized judgments.

Bias. Eliminating legally protected categories such as race and gender from the data fed into algorithms does not magically solve the problem of

120. Roberts, *supra* note 117, at 1708.

121. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/ND3T-B68Q]. The creator of COMPAS, Northpointe, defended its fairness, and this dispute has received wide coverage and analysis. *See, e.g.*, Mayson, *supra* note 113, at 2234–37.

122. Julia Dressel & Hany Farid, *The Accuracy, Fairness, and Limits of Predicting Recidivism*, 4 SCI. ADVANCES 1, 3 (Jan. 17, 2018), https://advances.sciencemag.org/content/4/1/eaao5580 [https://perma.cc/EV4G-CR73].

123. Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 813 (2014).

124. *Id.* at 839.

125. *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1368–71 (2018).

126. Berman, *supra* note 54, at 1331.

127. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1271–72 (2008).

bias, because those factors are associated with a range of other characteristics, which serve as proxies.[128] For example, race can be inferred from "neutral" data such as zip codes, media preferences, or certain names.[129] When Amazon rolled out same-day delivery service in twenty-seven metropolitan areas across America, it excluded certain zip codes that were largely African-American.[130] Amazon claimed that it did not consider race; rather, its algorithm was identifying zip codes with high concentrations of Prime members and areas closest to its warehouses.[131] Yet even without an intent to discriminate against minorities, the result was to disadvantage people who already suffer from a lack of convenient and quality retail in their neighborhoods.[132] Similarly, a study revealed that a commercial health care algorithm was identifying white patients for more intensive medical care than similarly ill black patients.[133] Why? The algorithm relied on data about past health care expenditures to make predictions about patients' future needs, but black people suffer barriers to health care access and thus have lower cost histories.[134] By reformulating the algorithm to eliminate cost as a proxy for needs, the racial bias disappeared.[135]

These examples demonstrate how developers can bake structural biases into algorithms, thereby "replicating real world inequalities"[136] even if they have no intent to discriminate. So, as in the prior example, if black patients have accrued lower health care costs over time, then the training data fed into algorithms designed to identify health care needs will replicate these

128. *See* Betsy A. Williams, Catherine F. Brooks & Yotam Shmargad, *How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications*, 8 J. INFO. POL'Y 78, 86, 90 (2018). The authors assert that social category data can be used productively to uncover biases. *Id.* at 79 ("When such sensitive information is used responsibly and proactively, ongoing discrimination can be made transparent through data-checking processes.").

129. "When aiming to prevent race discrimination, for example, one may find that a host of attributes in the United States correlate in some way with race. Some of those may be unexpected, and some of those may be legitimate considerations for the decision." Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1415 (2019); *see also* Hurley & Adebayo, *supra* note 93, at 193.

130. David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERG (Apr. 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day/index.html [https://perma.cc/8R9N-ZHHX].

131. *Id.*

132. *Id.* After this disparity was revealed in the media, Amazon responded by including those zip codes into the same-day delivery service. *Id.*

133. Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCI. 447, 450 (2019).

134. *Id.* at 447.

135. *Id.* at 453.

136. *See* Chander, *supra* note 49, at 1039 (advocating for increased transparency for algorithmic inputs and outputs).

discriminatory trends.[137] (Training data is the subset of data fed into an algorithm to teach the computer how to process information).[138] Because human beings code software,[139] developers can import their own unconscious biases into the collection and selection of data—such as using training data sets that are incomplete or that reflect structural inequities.[140] Bias can also creep into algorithms when developers frame the desired outcomes of the algorithm and when they select the features that the algorithm considers, both of which necessarily involve value judgments.[141] Tal Zarsky explains that

> at some points, analysts must decide which correlations and patterns should be incorporated into the scoring model and which must be set aside as 'junk,' random results, or statistical errors. Here, the analyst's biases might shape the final outcome and the discriminatory effect it will involve."[142]

Moreover, because software engineers are primarily white men,[143] these judgments may be unintentionally skewed due to a circumscribed worldview. As Cathy O'Neil succinctly states, "Models are opinions embedded in mathematics."[144]

B. Dirty Data and Careless Coding

Layered on top of these coding problems are widespread inaccuracies in the data that developers select and feed into algorithms. We know a lot about errors in credit reporting, because it is a regulated industry. In one study, the FTC found that twenty percent of consumers identified mistakes in their credit reports and that five percent of those reports contained errors serious

---

137. *See* Lillian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 28 (2017).

138. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 680 (2016).

139. Lehr & Ohm, *supra* note 48, at 660–61 (stressing the need for lawyers and policymakers to recognize how humans shape machine learning systems).

140. Barocas and Selbst explain in detail the mechanisms by which data mining can result in employment discrimination. Barocas & Selbst, *supra* note 138, at 677–93.

141. Karen Hao, *This Is How AI Bias Really Happens—and Why It's So Hard to Fix*, MIT TECH. REV. (Feb. 4, 2019), https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/ [https://perma.cc/H9DC-6MMM].

142. Tal. Z. Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375, 1391 (2014).

143. *See* Waldman, *supra* note 24, at 615.

144. O'NEIL, *supra* note 14, at 21.

enough to lead to denials of credit or higher rates.[145] These errors fall disproportionately on low-income consumers, who end up paying "higher interest rates [at] less favorable terms."[146] As a result, "[s]cores can become self-fulfilling prophecies, creating the financial distress they claim merely to indicate."[147] Although there is a statutorily-mandated process to correct credit reporting errors, it has been described as "Kafka-esque" due to its complexity and non-responsiveness by the credit reporting agencies.[148] Data inaccuracies are even worse in the data broker industry, which operates without regulation or any legally-mandated processes for transparency or correction.[149] Throughout the networked big data system, data errors are rife.[150]

Algorithmic decision-making, with its attendant biases and inaccuracies, also extends to government agencies, which interact extensively with low-income people.[151] Across the country, social service agencies are using automated systems, both created in-house and purchased from private vendors, to determine program eligibility and track compliance.[152] Automated

---

145. Press Release, Fed. Trade Comm'n, In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports that Could Result in Less Favorable Terms for Loans (Feb. 11, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports [https://perma.cc/FZ9B-UR2F]; *see also* Luke Herrine, *Credit Reporting's Vicious Cycles*, 40 N.Y.U. REV. L. & SOC. CHANGE 305, 321 (2016) (stating there are "more damaging errors for individuals with lower credit scores").

146. Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, Remarks at the CDIA Law & Industry Conference 4 (June 5, 2019), https://www.ftc.gov/system/files/documents/public_statements/1525705/slaughter_-_remarks_at_2019_cdia_law_industry_conference_6-5-19.pdf [https://perma.cc/4A4E-3E8N].

147. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 18 (2014).

148. *See* CONSUMER FIN. PROT. BUREAU, SUPERVISORY HIGHLIGHTS CONSUMER REPORTING SPECIAL EDITION 10–11 (2017), https://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf [https://perma.cc/QH7T-97SQ]; CHI CHI WU, MICHAEL BEST & SARAH BOLLING MANCINI, AUTOMATED INJUSTICE REDUX 7, 13 (2019), https://www.nclc.org/images/pdf/credit_reports/automated-injustice-redux.pdf [https://perma.cc/XY5E-6EZW]; Letter from Americans for Financial Reform et al. to Maxine Waters, Chairwoman, House Fin. Servs. Comm. 1 (Dec. 9, 2019), http://ourfinancialsecurity.org/wp-content/uploads/2019/12/2019.12.9-Support-letter-for-Protecting-Your-Credit-Score-Act-Gottheimer.pdf [https://perma.cc/QWQ2-P3P3].

149. *See* John Lucker, Susan K. Hogan & Trevor Bischoff, *Predictably Inaccurate: The Prevalence and Perils of Bad Big Data*, 21 DELOITTE REV. (July 31, 2017), https://www2.deloitte.com/us/en/insights/deloitte-review/issue-21/analytics-bad-data-quality.html [https://perma.cc/936U-3U8A].

150. Sharona Hoffman, *Big Data Analytics: What Can Go Wrong*, 15 IND. HEALTH L. REV. 227, 230 (2018) (on errors in health data); Valentine, *supra* note 16, at 388.

151. Citron, *supra* note 127, at 1267.

152. *Id.* at 1263–64.

decision-making has the potential to streamline access to services and improve accuracy, but in some jurisdictions, the promise has been outweighed by the peril.[153] For instance, in the Medicaid context, several states are adopting algorithms to determine levels of care for the disabled, elderly, and poor.[154] In their wake, thousands of disabled people have faced reductions and terminations in aid and services without any explanation from their state or opportunities for human intervention.[155] These technologically-driven tragedies, which extend to welfare, food stamps, and other public benefits programs, can be traced to the building of the algorithms.[156] Danielle Citron explains that "[p]rogrammers routinely change the substance of rules when translating them from human language into computer code."[157] She describes programmers in Colorado who, over a three-year period, inaccurately translated at least nine hundred state regulatory requirements into code, leading to hundreds of thousands of erroneous decisions, including improper denials of health care to pregnant women, women with breast and cervical cancer, and foster children, as well as improper denials of food stamps to the disabled.[158] Such problems extend far beyond Colorado.[159]

In Idaho, a class action suit was filed after disabled people saw their benefits slashed by as much as forty-two percent and could not get the state to explain its reasons or process.[160] It turns out that, among other problems, the state's algorithmic model for apportioning funds was trained on and using flawed and erroneous data.[161] In Arkansas, a similar class action lawsuit proved that the state's algorithm for determining Medicaid eligibility was rife with coding errors, such as inadvertently leaving out diabetes and improperly weighing the severity of cerebral palsy, prompting the lead legal aid attorney

153. Valentine, *supra* note 16, at 378 ("The predictive algorithm systems that governments rely on do not work as advertised and are far from infallible.").

154. *See* Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1275–79 (2020).

155. *See* EUBANKS, *supra* note 45, at 39–83; Citron, *supra* note 127, at 1268–77.

156. *See* Lehr & Ohm, *supra* note 48, at 669–701 (describing eight steps involved in machine learning and where programmers can go wrong).

157. Citron, *supra* note 127, at 1254.

158. *Id.* at 1256, 1268–69.

159. *Id.* at 1270–71 (discussing similar errors in California and Texas); Valentine, *supra* note 16, at 372–73 (discussing public benefits problems in New York City and Michigan).

160. Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, VERGE (Mar. 21, 2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy [https://perma.cc/NC7Y-GX7M].

161. FRY, *supra* note 34, at 17 ("[T]he data was so badly riddled with bugs and errors that it was, for the most part, entirely useless"); Lecher, *supra* note 160.

to query, "If states are using something so complex that they don't understand it, how do we know that it's working right? What if there's errors?"[162]

And, once algorithms are up and running, these problems are compounded by computer system failures;[163] reductions in staff;[164] lack of caseworker training;[165] decentralized case oversight;[166] loss of verification documentation provided by claimants;[167] pressures on case workers to close cases in order to meet performance metrics;[168] processing delays;[169] lack of adequate notice to claimants, who are thus denied the chance to object or appeal;[170] incorrect instructions to clients;[171] and decentralized case oversight.[172] Poor people face extreme surveillance in public benefits systems, but it is a one-way street with inadequate oversight over the government's use of algorithmic decision-making.

Algorithms are also compounding the consequences of poverty. For instance, child welfare agencies are increasingly using predictive software to determine which claims of child neglect or abuse to investigate further and which to drop.[173] These algorithms are more likely to sweep low-income families into their orbit, because they incorporate and emphasize data generated from programs associated almost exclusively with poor people, such as public benefits receipt and interaction with juvenile probation and youth services.[174] By contrast, middle class families gather family support privately, from therapists, doctors, private rehabilitation programs, and nannies and babysitters. This is the "missing" data that never gets fed into child welfare algorithms. Not surprisingly, the predictions generated from these algorithms are inaccurate, with high rates of false positives, which can devastate families when children are torn from their parents.[175]

Virginia Eubanks names these government surveillance technologies "the digital poorhouse"; it's a place where "poor and working-class people are targeted by new tools of digital poverty management and face life-threatening

---

162. Lecher, *supra* note 160.
163. EUBANKS, *supra* note 45, at 49, 63.
164. Valentine, *supra* note 16, at 391.
165. EUBANKS, *supra* note 45, at 50, 63.
166. *Id.* at 61–62.
167. *Id.* at 50.
168. *Id.*
169. *Id.* at 53.
170. *Id.* at 54.
171. *Id.* at 71.
172. *Id.* at 61–62.
173. *Id.* at 127–73.
174. *Id.* at 146–47, 156–57; Valentine, *supra* note 16, at 385.
175. *See* Valentine, *supra* note 16, at 380–81.

consequences as a result."[176] It is a place where technology obscures governmental decision-making and strips people's ability to understand or challenge the forces that control their lives.

C. Surveillance

Algorithms underlie a wide range of surveillance systems. Facial recognition technology, which uses machine learning algorithms to identify distinctive details about a person's face in order to match them within an existing database,[177] is expanding. Law enforcement agencies are using facial recognition, typically without notice to the public or local lawmakers, to identify arrestees by matching their photos with those contained in multiple databases, such as drivers' license records, mugshots, and social media.[178] Over half of American adults are in law enforcement facial recognition databases.[179] At the same time, there are growing commercial applications for facial recognition, such as in stores and stadiums, which employ the technology to enhance security and to learn more about consumers.[180]

In 2019, a landlord of a building serving low-income tenants in New York decided to replace keys with facial recognition software, thus angering residents who were concerned that the landlord would share their data with the police and use the data to push out tenants in order to gentrify the property.[181] Public housing authorities are similarly adopting facial

176. EUBANKS, *supra* note 45, at 11.

177. Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1596 (2017).

178. Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. U. L. REV. 1595, 1604 (2016); Jennifer Valentino-DeVries, *How the Police Use Facial Recognition and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/Y4NP-6FZ3].

179. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/2PPG-AQW7].

180. *See* Jeff John Roberts, *The Business of Your Face*, FORTUNE (Mar. 27, 2019), https://fortune.com/longform/facial-recognition/ [https://perma.cc/KN2S-SZBS].

181. Ultimately, the landlord dropped the plan, and several of the residents are advocating for legislative bans on the technology. *See* Alfred Ng, *Tenants Call for Better Laws After Stopping Facial Recognition from Moving In*, CNET (Nov. 22, 2019), https://www.cnet.com/news/tenants-call-for-better-laws-after-stopping-facial-recognition-from-moving-in/ [https://perma.cc/VL3Y-NL69]. *See also* Erin McElroy, *Disruption at the Doorstep*, URB. OMNIBUS (Nov. 6, 2019), https://urbanomnibus.net/2019/11/disruption-at-the-doorstep/ [https://perma.cc/UV3F-37M6]. McElroy discusses the rise of "proptech" in which real estate technology companies are impacting the "provision, consumption, and management of residential space." *Id.*

recognition, ostensibly to enhance security, while making the daily activities and movements of low-income, minority people available to law enforcement.[182] High-income residents have been more welcoming of facial recognition technology for the sense of security it provides and the gee-whiz nature of new technology.[183] Yet low-income tenants are more wary because they face more serious consequences from surveillance, such as eviction and entanglement with the criminal justice system.[184] This highlights how the same technology can have differential impacts on different groups—a comparison aptly described as luxury surveillance versus imposed surveillance.[185]

Facial recognition technology has also been used to target people of color who are engaging in constitutionally protected speech. During the 2015 protests in Baltimore City over the death of Freddie Gray while in police custody, the Baltimore City Police Department used facial recognition technology to identify and arrest protesters based on their social media postings.[186] Such surveillance impinges on Americans' right to freedom of assembly,[187] and it disproportionately impacts people of color.[188] It also flips democratic accountability, "with the supervisor now the supervised," which in turn "harms individuals' perceptions of themselves as citizens in a

182. *See* Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html [https://perma.cc/6GS3-RYD5].

183. Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. TIMES (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html [https://perma.cc/2UHS-MTJU].

184. *See* Chris Gilliard, *The Two Faces of the Smart City*, FAST COMPANY (Jan. 20, 2020), https://www.fastcompany.com/90453305/the-two-faces-of-the-smart-city [https://perma.cc/2P7X-2WWN]; McElroy, *supra* note 181 (noting that "real estate and technology platforms [proptech included] often work in conjunction to displace and target poor and working class tenants of color").

185. Gilliard, *supra* note 184.

186. Benjamin Powers, *Eyes over Baltimore: How Police Use Military Technology To Secretly Track You*, ROLLING STONE (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/ [https://perma.cc/LC5N-4KVT]; *see* Sidney Fussell, *The Strange Politics of Facial Recognition*, ATLANTIC (June 28, 2019), https://www.theatlantic.com/technology/archive/2019/06/democrats-and-republicans-passing-soft-regulations/592558/ [https://perma.cc/73G6-KXWZ].

187. Crump, *supra* note 178, at 1644 ("Surveillance technology may go beyond deterring conduct that is unlawful and inhibit or deter the legal and beneficial activities that citizens conduct in a free society.").

188. Powers, *supra* note 186. Powers also describes how the Baltimore City Police Department deployed aerial surveillance cameras attached to planes for months without alerting the city's citizens or local lawmakers.

democratic society."[189] Poverty already depresses democratic participation, thus feeding a growing economic divide as laws are passed to benefit the wealthy, while leaving poor Americans behind.[190]

Further, facial recognition technology is problematic for its lack of accuracy, especially for women and people of color. For instance, researchers Joy Buolamwini and Timnit Gebru found an error rate of up to 34.4 percent points higher for darker skinned females than lighter skinned males, raising the risk of wrongful arrests and mistaken identity.[191] But even as the software becomes more accurate,[192] the technology remains largely unregulated, does not require reasonable suspicion before police access it, lacks protections against misuse, and usually operates without public knowledge.[193] A few states and cities have passed laws limiting the use of facial recognition, and there is increasing bi-partisan support to regulate the technology,[194] but it remains legal in the vast majority of jurisdictions and for unlimited purposes.[195]

---

189. Craig Konnoth, *An Expressive Theory of Privacy Intrusions*, 102 IOWA L. REV. 1533, 1570 (2017).

190. Daniel Weeks, *Poverty vs. Democracy in America*, ATLANTIC (Jan. 6, 2014), https://www.theatlantic.com/politics/archive/2014/01/poverty-vs-democracy-in-america/282809 [https://perma.cc/MTE3-XN4J].

191. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 1, 8 (2018). Likewise, the ACLU conducted a study of Amazon's facial recognition tool that falsely identified twenty-eight members of Congress as criminals based on matching their faces with a mugshot database, and representatives of color were far more likely to be subject to the false match. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/5WCH-N59L].

192. Increased accuracy is not inevitable because larger datasets heighten the odds of people matching with other people. Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, ELECTRONIC FRONTIER FOUND. (Feb. 12, 2018), https://www.eff.org/wp/law-enforcement-use-face-recognition#_idTextAnchor005 [https://perma.cc/4PEJ-LC3D].

193. Garvie et al., *supra* note 179; George Joseph & Kenneth Lipp, *IMB Used NYPD Surveillance Footage To Develop Technology that Lets Police Search by Skin Color*, INTERCEPT (Sept. 6, 2018), https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/ [https://perma.cc/4RP4-43DJ].

194. Fussell, *supra* note 186.

195. The Illinois Biometric Information Privacy Act, which applies only to private companies, requires consumer consent and public notice about collection and sharing of biometric data. Stuart D. Levi et al., *Illinois Supreme Court Holds that Biometric Privacy Law Does Not Require Actual Harm for Private Suits*, SKADDEN (Jan. 29, 2019), https://www.skadden.com/insights/publications/2019/01/illinois-supreme-court [https://perma.cc/SE5T-Z9T9]. Oklahoma prohibits the state from sharing biometric data with the federal government. *See* Mark Lerner, *Real ID and the Battle that Still Goes On in Oklahoma and Other States*, CONST. ALLIANCE (Dec. 15, 2014), https://constitutionalalliance.org/real-id-and-

Surveillance systems are also endemic in the workplace;[196] employers use them to improve productivity, cut costs, make management and personnel decisions, reduce employee theft and rule breaking, limit litigation, and protect proprietary information.[197] As technology advances, so does monitoring of employees.[198] In the workplace, employers monitor employees with tools such as thumb scans, identification badges, closed circuit cameras, geolocation tracking, sensors on tablets and vehicles, and software that can analyze employees' tones of voice and facial expressions.[199] Employers can also examine employees' internet browsing histories, social media usage, emails, phone calls, use of productivity apps, and keynote strokes.[200] Many employers offer wellness programs, which track employees' health and lifestyle choices, including their fertility and pregnancies, via fitness trackers and smartphone apps.[201] Moreover, algorithms shape the daily experiences of workers as they are monitored and then nudged to the business's desired

---

the-battle-that-still-goes-on-in-oklahoma-and-other-states/ [https://perma.cc/3ATB-PVJ9]. Oregon bars facial recognition in combination with body cameras. Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/ [https://perma.cc/24Z4-AAAD].

196. *See* Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 738–39 (2017); Alexandra Mateescu & Aiha Nguyen, *Explainer: Workplace Monitoring & Surveillance*, DATA & SOC'Y (Feb. 2019), https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf [https://perma.cc/8RS7-PACC].

197. *See* Michele E. Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1408 (2012); Alex Rosenblat, Tamara Kneese & Danah Boyd, Workplace Surveillance 1, 3–5 (Oct. 8, 2014) (unpublished manuscript), https://www.datasociety.net/pubs/fow/WorkplaceSurveillance.pdf [https://perma.cc/Z8ZN-E9Z9]; *see also The Latest on Workplace Monitoring and Surveillance*, AM. MGMT. ASS'N (Apr. 8, 2019), https://www.amanet.org/articles/the-latest-on-workplace-monitoring-and-surveillance/ [https://perma.cc/XZ7Y-K62X] (reporting that one quarter of employers have fired workers for misusing email and one third have fired workers for internet misuse).

198. Ajunwa et al., *supra* note 196, at 738.

199. *Id.* at 743–44; *see* Ellen Ruppel Shell, *The Employer-Surveillance State*, ATLANTIC (Oct. 15, 2018), https://www.theatlantic.com/business/archive/2018/10/employee-surveillance/568159/ [https://perma.cc/ANK8-FKAG]. On biometric surveillance in the workplace, see Mateescu & Nguyen, *supra* note 196, at 7–9.

200. Ajunwa et al., *supra* note 196, at 743–44.

201. *Id.* at 763; Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/ [https://perma.cc/A4W5-EPCW] (describing the new employer tools of "menstrual surveillance").

behaviors.[202] There can be serious consequences from workplace surveillance, including physical and mental health problems resulting from the stress of surveillance, a loss of worker dignity and sense of autonomy, chilling of collective action, discrimination, and lower wages.[203] Surveillance is most oppressive and widespread in the low-wage workforce, making it a key issue to economic justice.[204]

Children are also increasingly surveilled. School districts across the country are purchasing software that monitors students' social media and online activity, both inside and outside of school, in an attempt to increase school safety in the wake of mass violence incidents.[205] This raises concerns about suppression of student speech and self-development, as well as the consequences of misinterpretation of student slang, pop culture references, and non-English speakers.[206] Moreover, children of color already face higher levels of school discipline, which may be amplified by monitoring technology that could "disproportionately tag students of color as dangerous."[207] Meanwhile, there is no solid evidence that surveillance

---

202. *See* ALEX ROSENBLAT, UBERLAND: HOW ALGORITHMS ARE REWRITING THE RULES OF WORK 4 (2018) ("Drivers are supposedly free and independent, but Uber's rules, enforced by these algorithmic managers, significantly limit the opportunities for entrepreneurial decision making available to them.").

203. *See* Charlotte Garden, *Labor Organizing in the Age of Surveillance*, 63 ST. LOUIS U. L.J. 55, 65–67 (2018); Gilman, *supra* note 197, at 1408–09; Pauline T. Kim, *Data Mining and the Challenges of Protecting Employee Privacy*, 40 COMP. LAB. L. & POL'Y J. 405, 418 (2019); Nathan Newman, *Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace*, 85 U. CIN. L. REV. 693, 716–19 (2017).

204. Gilman, *supra* note 197, at 1400; Wendi S. Lazar & Nantiya Ruan, *Is There a Future for Work?*, 25 GEO. J. ON POVERTY L. & POL'Y 343, 351–52 (2018); Tracy L. Vargas, *Employees or Suspects? Surveillance and Scrutinization of Low-Wage Service Workers in U.S. Dollar Stores*, 20 J. LAB. & SOC'Y 207, 210, 208 (2017) ("[R]epressive forms of worker surveillance are most prevalent in non-unionized retail settings where labor organization is weak or absent, where work is disproportionately performed by 'unskilled' workers, women, minorities, and immigrants, and where job tasks can be easily measured.").

205. Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. Rev. 1673, 1680–98 (2019); Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, GUARDIAN (Oct. 22, 2019), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle [https://perma.cc/B8VN-YCE6]; Faiza Patel & Rachel Levinson-Waldman, *School Surveillance Zone*, BRENNAN CTR. FOR JUST. (Apr. 30, 2019), https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone [https://perma.cc/C3EC-R4JE].

206. Patel & Levinson-Waldman, *supra* note 205.

207. *Id.* For other forms of student tracking, see Heather Kelly, *School Apps Track Students from Classroom to Bathroom, and Parents are Struggling to Keep Up*, WASH. POST (Oct. 29, 2019), https://www.washingtonpost.com/technology/2019/10/29/school-apps-track-students-

technology improves student safety.[208] This is one of many ways in which the consequences of surveillance systems can fall most harshly on the poor.

D. Conclusion

A lack of data privacy enables heightened surveillance and sorting of low-income and other marginalized people. There are economic impacts, as people lose opportunities that are necessary for financial stability, such as housing, employment, mainstream financial services, and education, while facing higher levels of interaction with the criminal justice and child welfare systems. Marion Fourcade and Kieran Healy explain how digital sorting systems capture behavior and thus embed moral judgements of their subjects: "Bad luck in missing a payment, or good fortune in having a parent who will pay a bill, get coded as poor or wise personal choices. One's score falls or rises accordingly."[209] This classification economy also has dignitary harms, as people lose autonomy over their own lives and are manipulated towards the ends of profiteers. As one of the tenants protesting facial recognition said, "We're saying we don't want this; we've had enough. We should not feel like we're in a prison to enter our homes."[210]

While much modern data collection and surveillance is covert and invisible, low-income people are particularly subject to overt surveillance designed not only to observe them but also to let them know they are being watched, such as law enforcement and workplace cameras. This sort of intrusion "signals disrespect to its victims and suggests to others that the victim lacks social standing and regard relative to other groups and institutions in society."[211]

At its most extreme, surveillance systems are driving marginalized people underground, where they remain disconnected from services and supports that could otherwise assist them.[212] A prime example of this problem of hyper-invisibility due to extreme privacy befalls undocumented people in the United States.[213] Due to fears about the federal government's technologically-fueled surveillance dragnet, they are pulling children out of schools, declining

---

classroom-bathroom-parents-are-struggling-keep-up/?arc404=true [https://perma.cc/72JS-LDVU].

208. Beckett, *supra* note 205.

209. Fourcade & Healy, *supra* note 33, at 24–25.

210. Misra, *supra* note 18.

211. Konnoth, *supra* note 189, at 153.

212. *See* Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253, 254–55 (2018).

213. *Id.* at 261–65.

to go to hospitals, and not applying for food stamps and other public benefits for which they are eligible.[214] They are becoming invisible. In sum, low-income people live at both extreme ends of the digital privacy spectrum, and existing laws do little to help them calibrate their privacy needs.

III. THE GAPS IN AMERICAN PRIVACY PROTECTIONS

Unlike the EU, the United States lacks a comprehensive privacy law regime. Our privacy protections are scattered among constitutional provisions, statutes, and the common law, as this Part surveys. Overall, in America, privacy is considered a good rather than a right, and as a result,

> privacy from companies has come to be discussed as a commodity or a privilege that individuals should always have the prerogative to give up, while regulation that in any way inhibits their ability to do so is frequently decried as paternalistic and anti-innovation.[215]

This Part surveys the privacy law landscape in the United States as it relates to people with low socio-economic status.

A. Constitution

At the constitutional level, privacy rights have developed to promote individual autonomy in family and bodily integrity, but the Constitution is less protective of our personal data.[216] Given the government's power, combined with its extensive databases of personal information, a constitutional right to informational privacy—or the right to keep the government from collecting and disclosing our personal information—could be significant, particularly for poor people.[217] It could restrict and enhance safeguards for the extensive database sharing that occurs among federal agencies, states, and private entities. Yet the Supreme Court has never held that the Fourteenth Amendment protects informational privacy.[218] Rather, the Court has ruled that even if such a right exists, it was not violated under the facts of the handful of cases before it, largely because of adequate statutory

---

214. *Id.* at 264–65.

215. Barrett, *supra* note 28, at 1065–66. On the differences in philosophy between the U.S. and EU approaches, see generally Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017).

216. *See* Gilman, *supra* note 197, at 1417.

217. *See* Danielle Keats Citron, Comment, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1156 (2018).

218. NASA v. Nelson, 562 U.S. 134 (2011); Whalen v. Roe, 429 U.S. 589 (1977).

protections against disclosure in those cases.[219] Thus, any defined constitutional right to informational privacy will have to wait until a later date.[220]

The Fourth Amendment is another potential bulwark against the government's collection and use of personal data; it protects citizens from unreasonable government searches and seizures.[221] Under the reasonableness touchstone, the Court has long held that objectively reasonable expectations to privacy are shed when people voluntarily share information with third parties (the "third-party" doctrine)[222] or in public.[223] Thus, sending emails or stepping outside your front door waives any reasonable expectation to privacy.[224] In a shift from this doctrine, the Court ruled in 2018 in *Carpenter v. United States* that a warrantless police search of cell phone site data violated the Fourth Amendment.[225] In so doing, the Court acknowledged the tension between the third-party doctrine and emerging technologies, which government can use to track people's lives at a granular level, over lengthy periods of time.[226] The Court ruled that the third-party doctrine did not apply

---

219. *NASA*, 562 U.S. at 147; *Whalen*, 429 U.S. at 601–02.

220. Lower courts have been more receptive to information privacy claims based on the Constitution. Citron, *supra* note 217, at 1150. At the same time, data processors have turned to the First Amendment and constitutional standing doctrine to argue for the free flow of data. Schwartz & Peifer, *supra* note 215, at 134–35.

221. U.S. CONST. amend. IV. The purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting Camara v. Mun. Court, 387 U.S. 523 (1967)).

222. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

223. Katz v. United States, 389 U.S. 347, 351 (1967). For analysis, see Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 570–71 (2017). For subsequent Supreme Court cases struggling to adapt its Fourth Amendment jurisprudence to emerging technologies, see Riley v. California, 573 U.S. 373, 386 (2014) (holding that the Fourth Amendment requires police to obtain a warrant to search a smartphone incident to arrest); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that warrantless police placement of GPS on suspect's car for twenty-eight days violates the Fourth Amendment under a trespass theory); Kyllo v. United States, 533 U.S. 27, 35–37 (2001) (holding that a warrant is required for use of a thermal imaging camera on a home).

224. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 526 (2006) (explaining that under the Court's third-party doctrine "if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information."). The result of the third-party doctrine is that it "undermines Fourth Amendment protection for most data trails." Ferguson, *supra* note 223, at 576.

225. *Carpenter*, 138 S. Ct. at 2223.

226. *Id.* at 2219–20.

to cell phone site data because cell phones are a necessity of modern life, and users have no choice in being tracked.[227]

The reach of *Carpenter* beyond its narrow context remains to be seen.[228] Is there a reasonable expectation that government will not access data held in commercial databases given the notice-and-consent regime that currently governs personal data?[229] How broad is the Court's notion of voluntary consent? Unfortunately, the Court has long held that poor people give up their reasonable expectations to privacy, even in their homes, when they seek governmental assistance.[230] If low-income people can lawfully be subject to investigatory home visits as a condition of receiving welfare benefits, it is hard to see how they can block government from accessing their data to manage public benefits regimes. Thus, the Fourth Amendment may serve a bulwark to deeply intrusive and warrantless uses of technology in police hands, but right now it probably has little to offer low-income people in terms of big data networks.[231]

B. Privacy Statutes

At the statutory level, American privacy laws are fragmented and sectoral, meaning they cover specific industries, such as health care providers or financial services companies, or specific forms of data, such as children's online activity.[232] Even within industries, these federal, sectoral laws are limited in their scope and effect,[233] and there is often a mismatch between their objectives and technological reality. "Privacy law is primarily concerned with causality, whereas Big Data is generally a tool of

---

227. *Id.*

228. Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (Oxford U. Press) (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 [https://perma.cc/KZ5H-6USK].

229. Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 230–31 (2018).

230. Wyman v. James, 400 U.S. 309, 313–25 (1971). For extended analysis of *Wyman*, see Michele E. Gilman, *Privacy as a Luxury Not for the Poor:* Wyman v. James (1971), *in* THE POVERTY LAW CANON (Ezra Rosser & Marie Failinger eds., 2016).

231. *See* Schwartz & Peifer, *supra* note 215, at 133.

232. *See* Barrett, *supra* note 28, at 1068; Schwartz & Peifer, *supra* note 215, at 136; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014); *cf.* Rustad & Koenig, *supra* note 10, at 381 (noting the benefits of a sectoral approach to be more tailored to specific risks).

233. *See* Barrett, *supra* note 28, at 1069.

correlation."[234] Three examples of major consumer-oriented privacy laws are illustrative.[235]

HIPPA protects patient health information collected by health care providers such as doctors,[236] but health information shared outside covered contexts remains fair game for data brokers and other end users.[237] That is why a search for "diabetes" on Google can ultimately result in a person paying a higher health insurance premium, why marketers can target sick people with advertising, or why a hospital can rely on a credit report to predict a patient's compliance with a medication regime.[238]

In the financial realm, the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to explain their information-sharing practices to customers and to safeguard sensitive data.[239] However, consumers must affirmatively opt out if they do not want their information shared.[240] This puts the onus on individuals to protect their privacy,[241] which can be challenging

234. Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework To Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 108 (2014).

235. For an overview of the various American privacy laws that govern the private sector, see CONG. RESEARCH SERV., *supra* note 27; Neil M. Richards, Andrew B. Serwin & Tyler Blake, *Understanding American Privacy*, *in* RESEARCH HANDBOOK ON PRIVACY & DATA PROTECTION LAW: VALUES, NORMS AND GLOBAL POLITICS (Gloria González Fuster, Rosamunde van Brakel & Paul De Hert eds.) (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256918 [https://perma.cc/7L9H-DL6N]; Shawn Marie Boyne, *Data Protection in the United States*, 66 AM. J. COMP. L. 299 (2018).

236. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in various sections of Titles 18, 26, 29, and 42 of the United States Code).

237. *See* Mary F.E. Eberling, *Uncanny Commodities: Policy and Compliance Implications for the Trade in Debt and Health Data*, 27 ANNALS HEALTH L. 125, 128 (2018); Pasquale & Ragone, *supra* note 106, at 629–30.

238. *See* Eberling, *supra* note 237, at 134–49.

239. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in Titles 12 and 15 of the United States Code). The Act was signed into law in 1999 with the purpose "to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers." *See* H.R. REP. NO. 106-434 (1999) (Conf. Rep.).

240. S*ee* 15 U.S.C. § 6802(b)(1) (2018).

241. *The Gramm-Leach-Bliley Act*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/glba/ [https://perma.cc/F3TG-UCAT]; *see also* Kathleen A. Hardee, *The Gramm-Leach-Bliley Act: Five Years After Implementation, Does the Emperor Wear Clothes?*, 39 CREIGHTON L. REV. 915, 926 (2006) ("Yet in the end, individual consumers have not yet realized any significant increase in protection from the handling, or mishandling, of their confidential financial information as a result of the GLBA."); Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230–32 (2002) (summarizing critiques of the Act).

given the complexity of the GLBA notices.[242] In addition, the GLBA permits sharing of personal data between corporate affiliates, which can include a large web of financial and non-financial businesses.[243] Furthermore, GLBA enforcement is entirely within the government's hands; there is no private right of action.[244] Meanwhile, companies like Facebook and Google are not financial institutions and can thus trade freely in financial information.[245]

The Fair Credit and Reporting Act aims to promote fairness, accuracy, and privacy in the consumer reporting industry.[246] These reports are used widely in lending, insurance, and housing contexts.[247] Consumers have rights under FCRA to view their reports and their credit scores, dispute incorrect or incomplete data, be advised when information has been used against them, and consent before reports are shared with employers.[248] However, data brokers largely evade FCRA's coverage, as do any household or neighborhood level determinations.[249] Moreover, while FCRA aims at ensuring the reporting of accurate information, it does nothing to protect against inaccurate inferences that end-users such as employers or landlords derive from reports.[250] It also does not protect information that employers gather directly from their workplace surveillance systems.[251]

---

242. *See* David Walrath, *Privacy and Information Disclosure: An Economic Analysis of the Gramm-Leach-Bliley Act*, 24 POL'Y PERSPECTIVES 55, 59–60 (2017).

243. Paul J. Polking & Scott A. Cammarn, *Overview of the Gramm-Leach-Bliley Act*, 4 N.C. BANKING INST. 1, 6 (2000).

244. *See* Borinski v. Williamson, No. Civ.A. 3:02–CV–1014, 2004 WL 433746, at *3 (N.D. Tex. Mar. 1, 2004); *see also* Lacerte Software Corp. v. Prof. Tax Serv., L.L.C., No. Civ.3:03–CV–1551–H, 2004 WL 180321, at *2 (N.D. Tex. Jan. 6, 2004).

245. *See* Barrett, *supra* note 28, at 1070. Further, many low-income people are unbanked, and thus this Act has little relevance to them in any event. *See* Kristin Johnson, Frank Pasquale & Jennifer Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499, 500–01 (2019) (noting that thirty-three million households in the United States are unbanked or underbanked).

246. 15 U.S.C. § 1681 (2018).

247. 15 U.S.C. § 1681(a).

248. *See* 15 U.S.C. §§ 1681g(a)(1), 1681g(c); 15 U.S.C. § 1681i(a)(1)(A).

249. *See* Hertza, *supra* note 87, at 1728–29; Hurley & Adebayo, *supra* note 93, at 186–87. The Act also excludes information compiled directly by a lender. Hurley & Adebayo, *supra* note 93, at 186–87.

250. *See* Kim, *supra* note 203, at 418; Madden et al., *supra* note 19, at 87. In addition, the Ninth Circuit concluded in 2019 in a ruling upholding a preliminary injunction in favor of a data broker that it could scrape data from public websites without violating the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018), which makes it a crime to access a computer "without authorization." HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1001 (9th Cir. 2019). The court ruled that a data broker that scraped data from LinkedIn was likely to succeed on the merits with the claim that it did not "circumvent[ ] a computer's generally applicable rules regarding access permissions." *Id.* at 1003.

251. Kim, *supra* note 203, at 417–18.

With regard to government-held data, the Privacy Act of 1974 is a code of fair information practices that governs how the federal government manages the information it holds about individuals.[252] The Act aims to restrict agency disclosure of personal data, to give individuals access to government records containing their information and the right to amend inaccurate or irrelevant records, and to establish norms for agency collection, maintenance, and dissemination of records.[253] However, the Act has numerous loopholes and has not kept pace with advances in modern technology, particularly given the massive sharing of information between public and private databases.[254] Also, while the Privacy Act and similar state analogues govern the government's storage and disclosure of information, they have not constrained the government's manner of collecting information from poor people in ways that are often stigmatizing and degrading, using methods such as intrusive questioning,[255] fingerprinting, and drug-testing as a condition of receiving public benefits.[256] The Privacy Act also contains an exception for nonconsensual disclosure of information to law enforcement; as a result, "when a population is imagined to be inclined toward criminality, then that population exists in a state of exception under the Privacy Act."[257] Data gathered from these intrusive practices is then fed into government databases and shared with state agencies, including law enforcement, leading to the further criminalization of poverty.[258] In sum, privacy statutes provide limited protections against emerging privacy harms and their associated economic injustices.

---

252. *See* 5 U.S.C. § 552(a) (2018).

253. U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 4 (2015 ed.) https://www.justice.gov/opcl/file/793026/download [https://perma.cc/P2WP-F5AV].

254. *See id.* at 1; Jonathan C. Bond, Note, *Defining Disclosure in a Digital Age: Updating the Privacy Act for the Twenty-First Century*, 76 GEO. WASH. L. REV. 1232, 1245–46 (2008).

255. *See* KHIARA M. BRIDGES, REPRODUCING RACE—AN ETHNOGRAPHY OF PREGNANCY AS A SITE OF RACIALIZATION 45–48 (2011); Jenna McLaughlin, *Pregnant, on Medicaid, and Being Watched*, INTERCEPT (Apr. 7, 2016), https://theintercept.com/2016/04/07/pregnant-on-medicaid-and-being-watched/ [https://perma.cc/29ZG-TEJU] (interviewing Khiara Bridges, who states what information patients must provide to access federalized, subsidized health care, including topics "from sexual abuse, to intimate partner violence, to how often they ate, what they ate, how they make their money, [and] how their partner makes their money.").

256. *See* Gilman, *supra* note 197, at 1422–23.

257. KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 161 (2017).

258. Gilman & Green, *supra* note 212, at 257; Kaaryn Gustafson, *The Criminalization of Poverty*, 99 J. CRIM. L. & CRIMINOLOGY 643, 674–78 (2009).

C. Notice and Consent

Outside of sectoral privacy statutes, the United States relies on self-regulation by companies that collect and use data and puts the burden on consumers to protect their own data.[259] This notice and consent approach seeks to provide consumers with information about a mobile app or website's privacy policy, including its collection, use, and sharing policies, in order to allow the consumer to decide whether or not to engage with the app or site.[260] Theoretically, this provides consumers with autonomy, while encouraging tech companies to innovate. Practically, however, it fails to protect consumers because it is founded on a myth of a fair contractual bargain between providers and consumers.

Numerous studies show that consumers do not read privacy policies because they are lengthy and rife with legalese and incomprehensible jargon.[261] This is an even greater challenge for less educated consumers, who are more likely to be low-income and who disproportionately—and mistakenly—trust that privacy policies will keep their data confidential.[262] Even the most diligent and highly educated consumer could not possibly read the multiple privacy policies connected to their daily online usage.[263] One study showed that it would take a person twenty-five days to read all the privacy policies that pop up in a year, with a national opportunity cost of $781

---

259. *See* Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261 (2014); Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S 485, 486–87 (2015); Solove & Hartzog, *supra* note 232, at 592.

260. *See* Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 374 (2014).

261. *See* Mark A. Graber, Donna M. D'Alessandro & Jill Johnson-West, *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. FAM. PRAC. 642, 642 (2002); Reidenberg et al., *supra* note 259, at 491; Sloan & Warner, *supra* note 260, at 391; Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 122–23 (2009); Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327, 1357–58 (2012).

262. Notice and consent are no barrier to discrimination; "[i]nstead, giving individuals notice and choice may simply perpetuate the growing gap between consumer 'haves' and 'have-nots' because the least sophisticated consumers remain least likely to protect themselves." Amy J. Schmitz, *Secret Consumer Scores and Segmentations: Separating "Haves" from "Have Nots*,*"* 2014 MICH. ST. L. REV. 1411, 1462–63 (2014); *see also* Thomas H. Koenig & Michael L. Rustad, *Digital Scarlet Letters: Social Media Stigmatization of the Poor and What Can Be Done*, 93 NEB. L. REV. 592, 616, 620, 627 (2015) (explaining that low-income persons can have lower levels of reading comprehension, rendering privacy notices useless).

263. *See* Reidenberg et al., *supra* note 259, at 492.

billion.[264] And even if consumers read and understood those polices, data collectors could still reserve the right to change their policies in the future without a new round of notice and consent.[265] Moreover, notice and consent policies do not give consumers control over how third parties use their data after buying it,[266] or how inferences about them are generated from data scraped by their social network "friends."[267]

Furthermore, data privacy policies are meaningless if they are breached. Notice and consent do nothing to forestall or remedy broken privacy promises, such as failure to adhere to the terms of a notice, negligent security practices, or wrongful retention of personal data.[268] Companies have tried to convince legislators and the public that they can effectively self-regulate, but the resulting internal processes often lack transparency, are drafted without input from consumers, are underfunded and short-term, and remain unenforced.[269] In addition, many companies refuse to implement even the most basic privacy protections.[270] For all these reasons, self-regulation can operate as a cover for companies to look as though they are attuned to consumers but is no substitute for substantive regulation.[271]

---

264. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S 543, 565 (2008).

265. *See* Danah Boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, 15 FIRST MONDAY 1, 2 (2010), https://firstmonday.org/article/view/3086/2589 [https://perma.cc/P37Z-KQGF]; Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 909 (2013) (describing how such privacy lurches, or changes in promised policies, "disrupt long-settled expectations"); Sprague & Ciocchetti, *supra* note 261, at 126.

266. *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 324 (2013); Natalie Kim, *Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 HARV. J.L. & TECH. 325, 327 (2014) ("[P]rivacy policies essentially remain a blunt instrument, giving users a binary option between sharing with none or sharing with all . . . ."); Reidenberg et al., *supra* note 259, at 492; Schmitz, *supra* note 262, at 1425.

267. Madden et al., *supra* note 19, at 87.

268. Reidenberg et al., *supra* note 259, at 521–23.

269. Robert Gellman & Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, WORLD PRIVACY F. 6 (2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf [https://perma.cc/8HK6-LJAJ]; *see also* Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY 15, 26 (2015) (concluding that membership in a self-regulatory body has no impact on privacy performance).

270. *See* Natasha Singer, *Consumer Groups Back Out of Federal Talks on Face Recognition*, N.Y. TIMES BITS BLOG (June 16, 2015, 12:10 AM), https://bits.blogs.nytimes.com/2015/06/16/consumer-groups-back-out-of-federal-talks-on-face-recognition/ [https://perma.cc/8CVE-UG99].

271. *See* Chris Hoofnagle, *Can Privacy Self-Regulation Work for Consumers?*, TAP BLOG (Jan. 26, 2011), https://www.techpolicy.com/Blog/January-2011/CanPrivacySelf-RegulationWork-for-Consumers.aspx [https://perma.cc/QQ5U-Q6YP].

D. Enforcement

For now, the Federal Trade Commission (FTC) is the United States' primary privacy enforcer,[272] with the job of holding companies to the promises they make in the notice-and-consent regime. The FTC enforces § 5 of the FTC Act, which declares unlawful "unfair or deceptive acts or practices," and which the FTC uses to fill the gaps left by the existing patchwork statutory approach to privacy.[273] Using this authority, the FTC has created a "common law" of privacy protections, in which it has taken enforcement actions against companies that violated their posted privacy policies, altered policies without consumer consent, made false representations to induce consumer consent, or failed to secure consumers' data.[274] Some FTC investigations have resulted in consent orders in which companies agree to implement measures to prevent future violations; these orders constitute a guide to best practices regarding permissible data uses that other companies rely upon.[275] However, this is a reactive, rather than proactive stance,[276] and it is further hobbled by limited firepower, with only forty full-time employees working on privacy issues.[277] Moreover, with regard to enforcement, the FTC cannot fine companies unless they violate an existing consent order, and fines have been "small in relation to the gravity of the violations."[278]

Effective enforcement also hinges on identifying privacy deprivations, yet much of the surveillance industry operates without consumers' knowledge. And, the industry wants to maintain that opacity. Algorithmic decision-making has been called a "black box" because of the complexity and lack of transparency around machine learning.[279] Attempts to breach the wall have been met with companies claiming non-disclosure agreements and trade secret protection for their software.[280] A criminal defendant in Wisconsin

---

272. *See* Rustad & Koenig, *supra* note 10, at 383.

273. *See* Solove & Hartzog, *supra* note 232, at 599, 621.

274. *Id.* at 628–40.

275. *Id.* at 607.

276. Barrett, *supra* note 28, at 1074.

277. Fred Cate, *74 Screens of Legalese Don't Protect Your Data—Here's a Blueprint for New Laws that Could Make a Difference*, CONVERSATION (Apr. 10, 2019), https://theconversation.com/74-screens-of-legalese-dont-protect-your-data-heres-a-blueprint-for-new-laws-that-could-make-a-difference-115101 [https://perma.cc/FD6N-GGTL].

278. Solove & Hartzog, *supra* note 232, at 605; *see also* Barrett, *supra* note 28, at 1076 (noting that the largest privacy fine imposed by the FTC was $22.5 million against Google, which is minor compared to the annual revenue of Big Tech companies).

279. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 4–8 (2015).

280. *See* Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 665–66 (2018).

named Eric Loomis attempted to gain access to the COMPAS system to understand, and challenge, his sentencing recommendation.[281] The Wisconsin Supreme Court upheld the denial of the defendant's request, holding that the risk assessment's underlying code could remain secret, partly because the algorithmic recommendation was a helpful factor, but not determinative, in the judge's decision-making.[282]

As the *Loomis* case demonstrates, in claims against the government for algorithmic transparency, individuals struggle to effectuate their due process rights to notice and a hearing.[283] The barriers are multiple: people are often unaware that a particular governmental or corporate decision was algorithm-generated; they may struggle to access information about the algorithm due to trade secret protections or government withholding of information; and if they are able to obtain information about an algorithm, they may be incapable of understanding its complexities.[284]

E. Anti-Discrimination Law

Current anti-discrimination law is similarly constrained in its potential to combat algorithmic inequality. Where discrimination is intentional, as in the Facebook advertising case, federal civil rights statutes can provide an effective remedy.[285] Of course, this requires that victims know they are the subject of discrimination—yet most people never know why they do not get a job interview or rental unit for which they applied. In addition to being invisible, much modern discrimination is unintentional and based instead on subconscious biases as well as historic patterns of structural inequality.[286] Thus, many discrimination cases hinge upon disparate impact theory, which makes neutral policies or practices unlawful if they have differential impacts on protected groups.[287]

---

281. Wisconsin v. Loomis, 881 N.W.2d 749 (Wis. 2016), *cert. denied*, 137 S. Ct. 2209 (2017).

282. *Id.*

283. *Id.*

284. Outside the criminal context, some courts have rejected trade secret claims in favor of plaintiffs' due process rights. *See* Valentine, *supra* note 16, at 418 (urging advocates to aggressively challenge trade secret claims).

285. *See infra* text accompanying notes 286–92; *see also* Rieke & Yu, *supra* note 29.

286. Barocas & Selbst, *supra* note 138, at 691, 698. *See generally* Linda Hamilton Krieger & Susan T. Fiske, *Employment Discrimination Law: Implicit Bias and Disparate Treatment*, 94 CALIF. L. REV. 997 (2006); Susan Sturm, *Second Generation Employment Discrimination: A Structural Approach*, 101 COLUM. L. REV. 458 (2001).

287. Barocas & Selbst, *supra* note 138, at 701. Disparate impact theory is available in cases brought under Title VII of the Civil Rights Act of 1964 (governing employment law), the Fair

Solon Barocas and Andrew Selbst have explained why disparate impact theory is ill-fit for combatting digital discrimination in employment under Title VII of the Civil Rights Act of 1964.[288] Algorithmic models analyze massive amounts of data that can be highly predictive of job performance; thus, courts permit employers to use them to match potential employees with job-related hiring criteria.[289] At the same time, due to the opacity of algorithms, plaintiffs struggle to identify alternative employment practices that achieve the same goals of accuracy while being less discriminatory, as Title VII requires.[290] Similar barriers to disparate impact cases arise in other contexts—a situation recently made worse when the Department of Housing and Urban Development announced proposed regulatory changes that, if adopted, will undermine disparate impact theory in housing cases by allowing landlords to rely, without liability, on algorithms created by third parties.[291]

Moreover, it remains the case that poverty is not a protected class under any anti-discrimination laws, making it perfectly acceptable to discriminate on the basis of social class.[292] Poverty also limits people from accessing legal recourse for digital discrimination, in part due to a shortage of civil legal aid lawyers and overwhelmed public defenders in criminal cases.[293] In addition, companies are evading discrimination litigation by requiring employees and consumers to sign arbitration agreements that keep disputes out of court and

---

Housing Act, the Age Discrimination and Employment Act, and the Americans with Disabilities Act. *See* Bryan Casey, *Title 2.0: Discrimination Law in a Data-Driven Society*, 2019 J.L. & MOBILITY 36, 44 (2019), https://futurist.law.umich.edu/title-2-0-discrimination-law-in-a-data-driven-society/ [https://perma.cc/DCD9-2NCX] (noting that the law is unresolved as to whether disparate impact theory is available in Title II of the Civil Rights Act of 1964, which bans discrimination in public accommodations).

288. Barocas & Selbst, *supra* note 138, at 701–12. Disparate impact claims are difficult to win in the analogue world as well, for reasons ranging from the difficulties of assembling the necessary statistical proof to judicial biases against employment plaintiffs. *See* Madden, et al, *supra* note 19, at 91.

289. Barocas & Selbst, *supra* note 138, at 707–08.

290. *Id.* at 710–11.

291. HUD's Implementation of the Fair Housing Act's Disparate Impact Standard, 84 Fed. Reg. 42,854 (proposed Aug. 29, 2019).

292. Peterman, *supra* note 74, at 1301.

293. *See* LEGAL SERVICES CORP., THE JUSTICE GAP: MEASURING THE UNMET CIVIL LEGAL NEEDS OF LOW-INCOME AMERICANS 6 (2017), https://www.lsc.gov/sites/default/files/images/TheJusticeGap-FullReport.pdf [https://perma.cc/X7DF-Z9EV] ("86% of the civil legal problems reported by low-income Americans in the past year received inadequate or no legal help."); NORMAN LEFSTEIN, SECURING REASONABLE CASELOADS: ETHICS AND LAW IN PUBLIC DEFENSE 8 (2012), https://www.americanbar.org/content/dam/aba/publications/books/ls_sclaid_def_securing_reasonable_caseloads_supplement.pdf [https://perma.cc/J2M7-B5DY] (discussing the excessive caseloads for public defenders and lack of sufficient funding).

shrouded in secrecy, while also forbidding employees from joining collectively to challenge discrimination.[294]

Finally, discrimination law covers only a subset of the technological harms impacting low-income people. The ability to obtain a low-skill job with a living wage, predictable hours, health care benefits, and affordable childcare is not solely a matter of purging discriminatory employers from the workplace. There is an entire sector of our economy that exploits workers regardless of their race, ethnicity, or gender. Likewise, there is not enough affordable housing in the United States, and thus getting rid of discriminatory lenders and landlords can reduce segregation, but it will not solve the structural problem of supply and demand. Public benefit systems serve only poor people, so a welfare movement that asks to be treated the same as the rich is meaningless to the social service bureaucracy. In other words, digital deprivations prey upon structural divisions within our economy. Illegal discrimination magnifies these disparities, but equality doctrine alone cannot lead to equity. Non-discrimination law serves the goal of equality, which is about treating people the same. By contrast, equity is about giving people what they need to be successful. Because discrimination law is not about fulfilling substantive guarantees to life's necessities, it can never do the heavy lifting of eliminating digital exploitation.

F. Workplace Protections

On the employment front, legal protections are equally scant. There are no federal laws securing employee privacy in the workplace.[295] State law protections, where they exist, are narrow. A few states protect employees from turning over their social media passwords to their bosses, and some require employee consent to electronic tracking, but these laws are narrow and scattered.[296]

Tort law does not prohibit most employer surveillance (or any form of surveillance).[297] There is a tort that protects against "intrusion upon seclusion," defined as an intrusion that would be "highly offensive to a

294. *See* Cynthia Estlund, *The Black Hole of Mandatory Arbitration*, 96 N.C. L. REV. 679, 680 (2018); Christopher R. Leslie, *The Arbitration Bootstrap*, 94 TEX. L. REV. 265, 270, 275 (2015).

295. Ajunwa et al., *supra* note 196, at 747; Kim, *supra* note 203, at 406.

296. Ajunwa et al., *supra* note 196, at 757, 758–59.

297. *See* Rustad & Koenig, *supra* note 10, at 385 ("Courts have largely been disinclined to stretch the tort of privacy to online surveillance and other Internet-related intrusions.").

reasonable person."[298] This is a high bar, and thus this tort prohibits only the most extreme and highly sensitive invasions of personal privacy in the workplace, such as cameras in locker rooms or bathrooms, and it provides no protection against the bulk of employer monitoring.[299] The common law privacy torts were created to protect elite members of society from public scrutiny, and thus not surprisingly, they hold no promise for low-wage workers or public benefit recipients.[300]

In sum, neither current American privacy laws nor anti-discrimination statutes currently have the teeth to secure data privacy or prevent digital discrimination. "In this legal universe, the rhetoric of bilateral self-interest holds sway."[301] Not surprisingly, there is an emerging consensus that America needs comprehensive privacy legislation.[302] There is less attention to the unique privacy needs and perspectives of low-income communities. The GDPR provides a starting point and model for considering data privacy protections.

IV. FIVE GDPR PRINCIPLES TO ADVANCE ECONOMIC JUSTICE

The GDPR went into effect in the EU on May 18, 2018.[303] The GDPR provides a unified privacy law framework for EU member-countries.[304] In contrast to U.S. privacy laws, the GDPR places multiple obligations on the entities that gather, hold, and use personal data (called "data controllers),[305]

298. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977). The other three common-law privacy torts are public disclosure of embarrassing private facts; publicity that places a person in a false light in the public eye; and commercial appropriation of a person's name or likeness. Gilman, *supra* note 197, at 1424. These have little application in the workplace and were initially developed to protect elite interests. *Id.* at 1425–26.

299. Gilman, *supra* note 197, at 1425–27; Kim, *supra* note 203, at 411–13.

300. Gilman, *supra* note 197, at 1426.

301. Schwartz & Peifer, *supra* note 215, at 132.

302. *See* U.S. GOV'T ACCOUNTABILITY OFF., INTERNET PRIVACY 31–33 (2019), https://www.gao.gov/assets/700/696437.pdf [https://perma.cc/AH6Z-EJ4P]. *See generally, e.g.*, Peter M. Lefkowitz, Opinion, *Why America Needs a Thoughtful Federal Privacy Law*, N.Y. TIMES (June 25, 2019) https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html [https://perma.cc/8NQG-4U5V]; Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/44SX-EMLB].

303. GDPR, *supra* note 1.

304. *See id.* at arts. 1–3. The GDPR permits derogations (or variations) on a country-by-country level on certain issues. *See id.* at arts. 85(2), 89(3).

305. GDPR, *supra* note 1, at art. 4(7). Personal data is defined as "any information relating to an identified or identifiable natural person." *Id.* at art. 4(1).

while also granting consumers (called "data subjects") rights to enhance their control over personal information.[306] The GDPR is based on the long-standing EU conception of privacy as a fundamental human right that constrains both government and private entities.[307] Whereas in the United States, data collection is freely allowed unless a specific law prohibits it; in the EU, a data controller can only collect data with a legally granted basis.[308] Under the GDPR, data subjects possess these core rights[309]:

- to be informed when data is being collected, including how and why it will be processed, along with a notice of rights,[310]
- to provide informed consent before personal data is processed,[311]
- to object or withdraw consent to processing of personal data, including the right to opt out of direct marketing,[312]
- to access personal data in an understandable format and in a timely manner,[313]
- to request correction of inaccurate or incomplete data,[314]
- to have personal data erased (the right to be forgotten),[315]
- to have personal data transferred from one service provider to another (the right to portability),[316]
- to obtain human intervention in significant decisions based on automated processing,[317] and

306. *Id.* at art. 4(1); *see also* Barrett, *supra* note 28, at 1083 (describing the GDPR's rights-based framework).

307. Schwartz & Peifer, *supra* note 215, at 123–26 (discussing history of privacy rights in the EU).

308. Barrett, *supra* note 28, at 1083; Schwartz & Peifer, *supra* note 215, at 120, 123; *cf.* Rustad & Koenig, *supra* note 10, at 368 (discussing the convergences between EU and U.S. approaches).

309. These rights are not absolute; rather, there are various exceptions and conditions, and application of the GDPR may require a balancing of interests when rights conflict. GDPR, *supra* note 1, at recital (4).

310. *Id.* at arts. 12–14.

311. *Id.* at arts. 6(1), 7.

312. *Id.* at arts. 7(3), 21.

313. *Id.* at art. 15(1).

314. *Id.* at art. 16.

315. *Id.* at art. 17.

316. *Id.* at art. 20.

317. *Id.* at art. 22.

- to demand an explanation regarding automated processing.[318]

With this combination of controller responsibilities and data subject rights, the GDPR seeks to vindicate principles of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[319]

The GDPR permits country-specific derogations on certain issues and contains unresolved textual ambiguities. Thus, many terms of the GDPR will gain further definition and content as the law is implemented and enforced over the coming years. Interpretive sources include the Recitals in the Preamble, guidance issued by the Article 29 Working Party (A29WP) (an advisory board of data protection authorities from across the EU), and the interpretations of member-country enforcement agencies.[320] Despite its ambiguities, the GDPR contains several provisions that have the potential—if enforced—to limit the big data harms to low-income and marginalized communities and, by enhancing transparency and accountability, to spur more targeted, substantive protections in the future. These five principles have the potential to advance economic justice: (1) the right to an explanation, (2) the right not to be subject to decisions based on automated profiling, (3) the right to be forgotten, (4) a requirement of public participation, and (5) robust implementation and enforcement.[321] Only time will tell if these provisions fulfill their potential to enhance the data privacy of vulnerable groups, but they provide an existing template for thinking about how to shape comprehensive privacy laws in the United States, at both the federal and state levels. Each one is discussed in turn.

A. Right to an Explanation

The "black box" of algorithmic decision-making hinders transparency, legibility, and accountability. The GDPR contains several provisions designed to open the box, including what has been popularly termed the

---

318. *Id.* at art. 15(1)(h).

319. *Id.* at art. 5.

320. *See* Bryan Casey, Ashkon Farhangi & Roland Vogl, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, 34 BERKELEY TECH. L.J. 145, 152–53 (2019); Talia B. Gillis & Josh Simons, *Explanation < Justification: GDPR and the Perils of Privacy*, 2 PA. J.L. & INNOVATION 71, 71 (2019); Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 193–95 (2019).

321. *See* GDPR, *supra* note 1, at arts. 13–15, 17, 22, 35, 77–84.

"right to an explanation."[322] Under the GDPR, entities that handle the personal data of EU citizens must "ensure fair and transparent processing" in automated decision-making by providing citizens with "meaningful information about the logic involved."[323] The scope of the GDPR's right to an explanation is hotly contested within the scholarly and technical communities.[324] One core question is whether the explanation should be about how the automated decision-making system was applied to a specific person, or whether it should describe how the system operates as a whole. Solon Barocas and Andrew Selbst frame this as a choice between "outcome-based" or "logic-based" explanations.[325] Outcome-based explanations focus on the facts that proved relevant to a particular machine-generated decision.[326] These explanations can potentially provide people with information necessary to correct errors or omissions, or to make a fix to their data to obtain goods or services (such as by changing their spending patterns to improve their credit rating). However, individualized explanations generally are not sufficient to uncover disparate impacts on certain groups or to solve structural problems that can be baked into algorithms.[327]

Accordingly, logic-based explanations might be necessary to ferret out digital discrimination. Such an explanation could reveal coding biases, improper interpretations of regulatory or business objectives, adverse impacts on particular groups, and other embedded problems in particular models.[328] The challenge with logic-based explanations is that they are often complex, if not inscrutable, to the layperson.[329] Even computer scientists and engineers can struggle to understand the machine learning mechanisms that they set in motion, because machine learning can be opaque, with "constellations of data . . . so complex that it's tough to retrace the line drawn by the

322. *Id.* at art. 71.

323. *Id.* at arts. 13(2), 14(2), 15(1). This right is set forth in Articles 13, 14, and 15, which require transparency in connection with automated decision-making, *id.* at arts. 13–15, as well as Article 22, which specifically concerns "automated individual decision-making, including profiling," *id.* at art. 22.

324. For summaries of the debate, see Casey et al., *supra* note 320, at 159–65; Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIVACY L. 233, 233–34, 237–39 (2017) (summarizing debate).

325. Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1099 (2018); *cf.* Edwards & Veale, *supra* note 137, at 55 (tracking the difference between model-centric versus subject-centric explanations).

326. Selbst & Barocas, *supra* note 325, at 1100.

327. *Id.* at 1105 (explaining that a single consumer cannot observe disparate impact, and an outcome-based explanation does not reveal why a system was constructed a certain way, which is necessary to prove disparate impact).

328. *See id.* at 1108–09.

329. *Id.* at 1093–94.

machine."[330] Providing laypeople with confusing explanations may technically comply with a regulatory command, but "[r]ights become dangerous things if they are unreasonably hard to exercise or ineffective in results, because they give the illusion that something has been done while in fact things are no better."[331] Moreover, people generally do not want a tutorial in machine learning methodology; rather, they want a decision in their favor, or at least guidance on how to secure one.[332]

Accordingly, Andrew Selbst and Julia Powles argue that any explanation must serve the instrumental value of being "at least meaningful enough to facilitate the data subject's exercise of her rights guaranteed by the GDPR and human rights law."[333] Similarly, Margot Kaminski calls for an explanation that "provide[s] enough information that an individual can act on it."[334] In other words, "the substance of the other underlying legal rights often determines" the nature of the right to an explanation."[335] The A29WP has issued guidance that reflects these insights, providing that "a complex mathematical explanation" is not necessary and instead defining "meaningful information about the logic involved" to include (1) the categories of data used in processing; (2) the relevance of the data; (3) how profiles are built; (4) the relevance of the profile to the decision-making process; and (5) how the profile is used for an individualized decision.[336]

The concept of an explanation for algorithmic decision-making is not foreign to American law. The United States has consumer statutes that give consumers the right to an outcome-based explanation with regard to unfavorable consumer reports that impact their access to credit, employment,

---

330. Dave Gershgorn, *We Don't Understand How AI Make Most Decisions, so Now Algorithms Are Explaining Themselves*, QUARTZ (Dec. 20, 2016), https://qz.com/865357/we-dont-understand-how-ai-make-most-decisions-so-now-algorithms-are-explaining-themselves/ [https://perma.cc/4JC3-AYXA]; *see also* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 638 (2017); Mike Ananny & Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, NEW MEDIA & SOC'Y (2016), https://journals.sagepub.com/doi/full/10.1177/1461444816676645 [https://perma.cc/UP7L-GPQD].

331. Lilian Edwards & Michael Veale, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, 16 IEEE SECURITY & PRIVACY 46, 50 (2018).

332. Edwards & Veale, *supra* note 137, at 42.

333. Selbst & Powles, *supra* note 324, at 236.

334. Kaminski, *supra* note 320, at 213.

335. *Id.*; *see also* Edwards & Veale, *supra* note 137, at 55–58.

336. *Article 29 Data Prot. Working Party Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, at 31, WP 251, (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826 [https://perma.cc/M92K-BGZ6] [hereinafter A29WP].

insurance, or housing.[337] The Fair Credit Reporting Act (FRCRA) and the Equal Credit Opportunity Act (ECOA) together seek to ensure that credit reports are fair, accurate, and non-discriminatory.[338] These laws require that individuals whose consumer reports are used adversely in lending, employment, insurance, or housing be issued an "adverse action notice."[339] In the credit context, the notices typically advise consumers which factors, from a pre-set checklist of twenty-four reasons, resulted in their adverse action; listed factors include "credit application incomplete;" "unable to verify credit references;" and "temporary or irregular employment" and the like.[340]

The FCRA/ECOA "explanation" is thus outcome-based. With the adverse action notice in hand, consumers supposedly have the opportunity to better understand decisions that impact them, to take steps to reverse the action, and to prevent discrimination.[341] Still, the FCRA explanation does not tell a person how or why the listed factor adversely impacted their score.[342] And it cannot effectively uncover disparate impact.[343] By contrast, the GDPR's requirement that controllers provide data subjects with information of the "logic involved" in a decision appears to envisage a broader, more detailed explanation about how the automated decision-making model operates.[344] In short, the GDPR is aimed at a "meaningful" explanation, and not a FCRA-style checklist, which can be illusory. At this time, it remains to be seen how EU enforcement authorities will interpret the "right to an explanation."

On this side of the Atlantic, policymakers should recognize that *both* outcome-based and logic-based explanations are warranted, depending on the circumstances, to advance data privacy that fosters non-discrimination and economic justice. We know that algorithms are impacting access to employment, education, housing, health care, financial services, insurance, consumer goods, electoral information, and public benefits in the United

337. *See* Selbst & Barocas, *supra* note 325, at 1099–1100.

338. 15 U.S.C. §§ 1681–1681x (2018) (FCRA); 15 U.S.C. §§ 1691–1691f (2018) (ECOA); *see also* Selbst & Barocas, *supra* note 325, at 1102. On the purposes underlying the statutes, see Shepard, *supra* note 87, at 1746 ("Congress's primary objective was to give consumers a meaningful participatory role in an otherwise ex parte 'trial' that had the potential to deprive a consumer of credit, insurance, and employment.").

339. 15 U.S.C. §§ 1681m, 1691(d)(2) (2018).

340. 12 C.F.R. pt. 1002 app. C (2018) (the sample notification form issued by the Federal Reserve Bank to satisfy the adverse action notification requirements).

341. Selbst & Barocas, *supra* note 325, at 1102.

342. *See* Hertza, *supra* note 87, at 1727.

343. Selbst & Barocas, *supra* note 325, at 1104–05.

344. *Id.* at 1107.

States.[345] We know far less about how algorithms are designed, the data that feeds them, the desired outcomes, or whether the models are accurate in meeting those outcomes. A statutory right to an explanation would provide much needed transparency around these issues. Transparency is foundational to accountability, which in turn "empowers those who might otherwise be powerless, demanding that those who wield power over them offer an account of their conduct."[346]

In some circumstances, an outcome-based explanation may be adequate to ensure that a system is operating fairly and in compliance with the law. For instance, a legal services lawyer could use a right to an explanation to benefit clients, without having to undertake onerous litigation. In the current "black box" environment, it is difficult to know why a client was denied a job or housing or public benefits or the like, or even if an algorithm was involved. Further, much litigation involving low-income people has no discovery or very limited discovery tools.[347] And even where discovery is available, it is a poor substitute for a right to an explanation, because it occurs only after cases are filed—and cases cannot be filed without a good faith basis to believe that wrongful conduct has occurred.[348] Thus, a right to an outcome-based explanation would open the algorithmic black box to scrutiny, allowing consumers to correct errors or omissions in their personal data; to request reconsideration; to explain why the algorithm is inaccurate or inappropriate given their personal situation; or to take steps to improve one's chance at meeting the algorithm's desired outcomes. On the technical side, computer scientists are devising explanatory systems that "translate" code into cognizable visualizations and interactions for laypersons, and research in this area is constantly evolving.[349] These tools can help low-income people and their advocates identify actionable claims, particularly since lawyers who represent low-income people typically lack resources for costly experts to help them understand and litigate scientific and technical material.

In other circumstances, it may be necessary to challenge an underlying model, such as when the algorithm inaccurately interprets the law or discriminates against protected groups. Consider Facebook's advertising

345. *See supra* Part II.

346. Gillis & Simons, *supra* note 320, at 76.

347. *See* BRITTANY K.T. KAUFFMAN, ALLOCATING THE COSTS OF DISCOVERY: LESSONS LEARNED AT HOME AND ABROAD 2–3 (2014), https://iaals.du.edu/sites/default/files/documents/publications/allocating_the_costs_of_discovery.pdf [https://perma.cc/L7LR-N3ZD].

348. *See* FED. R. CIV. P. 11.

349. Edwards & Veale, *supra* note 137, at 62–63; Kaminski, *supra* note 320, at 214; Selbst & Barocas, *supra* note 325, at 1114–17.

system, which was employing algorithms to allow advertisers to exclude women, older workers, minorities, and other defined groups from seeing certain ads in their feeds.[350] In such a situation, an individualized outcome-based explanation would not be adequate to dissemble the entire system.[351] In addition, there may be situations in which people question whether or not automated decision-making is appropriate for the setting at hand. Understanding how a model operates may help answer whether automated decision-making is a valid exercise of commercial or governmental power.

Thus, American law should require explanations not only for dissatisfied or curious individuals but also to regulatory experts and independent third parties with the technical chops to audit systems for accuracy, as well as "for noncompliance with values like equality, nondiscrimination, dignity, privacy, and human rights."[352] Audits are "the most prevalent social scientific method for the detection of discrimination" in machine learning systems.[353] The law can also require that algorithmic systems build in technical accountability, meaning software "that furnishes relevant evidence to support evaluation and . . . . assures that the subject of any such processes can determine that the rules and procedures have been followed."[354] Significantly, the GDPR's right to an explanation both contains "individual transparency rights" and a "systemic approach to algorithmic accountability."[355] The GDPR's systemic approach is accomplished in part through outside algorithmic audits by

350. *See supra* text accompanying notes 67–75.

351. Selbst & Barocas, *supra* note 325, at 1105 (arguing that a consumer's "single point of reference does not provide any understanding of the frequency of denials along protected-class lines, so she cannot observe disparate impact").

352. Waldman, *supra* note 24, at 630 (advocating for substantive audits in lieu of process-oriented proposals). "In addition, a system could be built to enable participants to check these properties for their own outcomes so that nontechnical users could verify these facts while the system as a whole would be overseen by others—potentially both inside and outside of government—who have the necessary technological expertise." Kroll et al., *supra* note 330, at 703.

353. Christian Sandvig et al., Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms 5 (May 22, 2014) (unpublished manuscript), http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf [https://perma.cc/QK2N-4HFU].

354. Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 44 (2018).

355. Kaminski, *supra* note 320, at 211; *see also* Edwards and Veale, *supra* note 137, at 77–80 (noting that the DPIA process can fulfill due process norms more effectively than individualized explanations).

government authorities and independent third parties, as well as through internal Data Protection Impact Assessments.[356]

In the GDPR, the right to an explanation is designed to improve the fairness, transparency, and accountability of algorithmic decision-making, and likewise in the United States, a right to an explanation should be shaped broadly and contextually to effectuate that objective. Explanations can help uncover digital discrimination and exploitation against the poor, improve the accuracy of automated decision-making systems that sort the poor and serve as gatekeepers to life necessities, and expose surveillance systems to public scrutiny. In all these ways, the right to an explanation can enhance economic justice.

B. Right to Object to Automated Profiling

Article 22 of the GDPR gives individuals the "right not to be subject to a decision based solely on automated processing, including profiling" when the decision produces "legal effects" or "similarly significant[ ] [e]ffects" on the individual.[357] In short, it ensures humans have recourse to human decision-makers on important decisions that impact their lives. Automated processing has serious consequences for low-income populations, who are more likely to be subject to algorithmic decisions and for whom the stakes are high. As Cathy O'Neil explains, "The privileged . . . are processed more by people, the masses by machines."[358] For example, "A white-shoe law firm or an exclusive prep school will lean far more on recommendations and face-to-face interviews than will a fast-food chain or a cash-strapped urban school district."[359]

The GDPR defines automated processing broadly with a nod toward the consequences of socioeconomic profiling. Its definition covers the processing of factors that can be used to segment people by social class and other categories. It applies to data used "to analyse or predict aspects concerning [a] natural person's performance at work, *economic situation*, health, personal preferences, interests, reliability, behaviour, location or

356. Kaminski, *supra* note 320, at 205–06.

357. GDPR, *supra* note 1, at art. 22(1). Article 22 contains three exceptions: (a) for processing necessary for performing a contract, (b) where the law permits it and there are safeguards for the data subject's rights, and (c) where the data subject has given explicit consent. *Id.* at art. 22(2).

358. O'NEIL, *supra* note 14, at 8.

359. *Id.*

movements."[360] Even when people consent to automated processing, which is a permissible basis for processing under the GDPR, a data controller must still provide "suitable measures to safeguard the data subject's rights," including "at least the right to obtain human intervention . . . to express [the data subject's] point of view and to contest the decision."[361] Moreover, some sensitive data are off the table for profiling altogether in the absence of explicit consent or other narrow, protective exceptions[362]: racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, sex life, sexual orientation, and genetic data.[363] The GDPR thus provides a backstop against algorithmic inferences and predictions about people that might not be accurate, fair, or appropriate.

There are three key questions about the scope of Article 22 that remain to be resolved as the GDPR is implemented: (1) how much human intervention takes a decision outside the scope of Article 22's protections? (2) what constitutes a decision with "legal" or "similarly significant" effect? and (3) does Article 22 ban these forms of automated processing altogether or instead provide data subjects with a right to opt out of such processing?[364] Each of these questions can be answered narrowly or broadly. Adopting the most privacy protective resolution to each of these open questions would enhance the economic mobility of low-income people.

To begin with, the GDPR recognizes the importance of keeping a human in the loop when automated decision-making is used. In many contexts, algorithmic outputs are not determinative on their own but are used to inform human judgments. Consider the COMPAS criminal sentencing algorithm in which a judge considers the algorithm's recommendation in assessing a defendant's likelihood of re-offense.[365] Here, the algorithm is supposed to inform the judge's decision-making and not to supplant it. This would not violate the GDPR's ban on solely automated decision-making. To be sure, there are concerns that judges are too deferential to algorithms because they

360. GDPR, *supra* note 1, at art. 4(4) (emphasis added).

361. *Id.* at arts. 7, 22(3).

362. Other exceptions are if the processing is necessary to perform a contract or is legally authorized, and there are "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." *Id.* at art. 22(2).

363. *Id.* at arts. 9(1), 22(4).

364. *See generally* Michael Veale & Lilian Edwards, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, 34 COMPUTER L. & SECURITY REV. 398 (2018).

365. *See supra* text accompanying notes 118–122.

see them as objective and infallible; this is the dilemma of automation bias.[366] Still, the judicial system keeps a "human in the loop" and provides mechanisms for advocacy and an adversarial process to contest the algorithmically-informed outcome. This judicial process would thus satisfy the GDPR's ban on solely automated processing, although risk prediction algorithms may well run afoul of constitutional due process and equal protection norms and be litigated on those grounds.[367] In other words, the transparency provided by a strong privacy law can be a foundation to seek accountability via other legal doctrines.

Consider, by contrast, an algorithm that sorts job applicants by predicting who is most likely to stay with the company long-term. A human resources employee who prints out a batch of applications meeting the algorithmic threshold and automatically sets up interviews with those candidates would not constitute meaningful human interaction. Thus, the company's decision to deny an interview to a person without any opportunities for an explanation or to challenge the decision would constitute a form of impermissible automated profiling.[368]

Of course, this right cannot possibly attach to every instance of automated decision-making; these tools touch almost every sector of the economy.[369] For this reason, Article 22 applies only to decisions with legal or similarly significant effects. The A29WP opines that significant decisions include those that affect financial circumstances, access to health services, access to education, or that deny employment.[370] These are all key elements of achieving economic stability.

By contrast, it is generally assumed that targeted advertising—even though it relies extensively on automated profiling—falls outside the scope

366. *See supra* text accompanying note 127; *see also* Angèle Christin, Alex Rosenblat & Danah Boyd, *Courts and Predictive Algorithms*, DATA & SOC'Y 8 (Oct. 27, 2015), https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf [https://perma.cc/UXS6-XDW2] (stating that an algorithm "seems more reliable, scientific, and legitimate than other sources of information," despite the reality that algorithmic quality varies immensely).

367. *See generally* Starr, *supra* note 123.

368. *See* Veale & Edwards, *supra* note 364, at 400 ("There is a strong argument therefore that rights to control 'solely' automated decision making must also apply to decisions made with *some* degree of human involvement . . . ."). These two examples only touch upon the wide range of human involvement in automated decision. *See generally* Kiel Brennan-Marquez, Karen Levy & Daniel Susser, *Strange Loops: Apparent Versus Actual Human Involvement in Automated Decision Making*, 34 BERKELEY TECH. L.J. 745 (2019).

369. Veale & Edwards, *supra* note 364, at 399.

370. A29WP, *supra* note 336, at 22.

of Article 22.[371] People may be annoyed or find it creepy to be followed around social media with sneaker advertisements after briefly viewing a Nike basketball shoe online,[372] but it will not likely have a significant impact on their life.[373] Nevertheless, some targeted ads are aimed at particularly vulnerable consumers in manipulative ways that can have serious consequences. Examples include advertising for payday loans and for-profit educational institutions, which are targeted to minority and low-income people but would rarely appear in the social media feed of a high-income earner.[374] Latanya Sweeney compared Google searches of female names associated with blacks (such as Latanya and Latisha) to searches of more typically white names (such as Kristen and Jill) and found that ads related to an arrest record appeared more frequently for the former than the latter.[375] This disparity could have detrimental effects if an employer is conducting a background check by searching an applicant's name, and it can also harm a person's self-identity and dignity regardless of the employment consequences.

Safiya Noble describes disturbingly sexist and racist content generated in response to internet searches of terms relating to minority groups and women.[376] For instance, when Noble conducted a Google search in 2011 of the term "black girls," the top results were links to pornography.[377] Such results compound race and gender profiling, "and even economic redlining," as discriminatory digital profiles control access to key resources and opportunities.[378] Noble explains that machine learning is not neutral; rather, it includes "decision-making protocols that favor corporate elites and the powerful."[379]

In this vein, the A29WP acknowledges that dignitary impacts on certain groups can be significant, stating that prohibited forms of solely automated processing include those that "have the potential to significantly affect the

371. *Id.*

372. *See* IGO, *supra* note 2, at 352 (discussing the framing of privacy concerns related to data collection practices).

373. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1029 (2014) (arguing "the experience is not a comfortable one" and is fairly described as "Kafkaesque").

374. O'NEIL, *supra* note 14, at 144.

375. Latanya Sweeney, *Discrimination in Online Ad Delivery*, CORNELL U. (Jan. 29, 2013), https://arxiv.org/abs/1301.6822 [https://perma.cc/MH4Q-LVC6].

376. SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 3–9 (2018).

377. *Id.* at 3.

378. *Id.* at 28.

379. *Id.* at 29.

circumstances, behavior or choices of the individuals concerned."[380] Significant effects thus must be judged by the intrusiveness of the profiling process, the expectations and wishes of the individuals concerned, the manner in which the ad is delivered, and the particular vulnerabilities of the data subjects targeted.[381] There are thus times when targeted advertisements may be impermissible.

Limitations on automated processing would help expand opportunities for low-income people in the United States. Despite America's identity as a socially mobile society, the reality is that most people's economic standing is determined by the parents to whom they are born.[382] Forty percent of children born in the bottom quintile of the income scale will remain there their entire lives; and the same is true of forty percent born in the top quintile.[383] The poverty rate is almost twelve percent, or 38.1 million people,[384] while millions more above the official poverty line struggle to meet basic needs.[385] Even in times of robust economic growth, growing economic inequality has continued unabated.[386] The top one percent earns sixteen percent of the nation's income and holds almost forty percent of its wealth,[387]

---

380. A29WP*, supra* note 336, at 21.

381. *Id.* at 22.

382. *See* ICELAND, *supra* note 43, at 62; Michele Gilman, *A Court for the One Percent: How the Supreme Court Contributes to Economic Inequality*, 2014 UTAH L. REV. 389, 407 (2014) (citing data and sources).

383. PEW CHARITABLE TRUSTS, PURSUING THE AMERICAN DREAM: ECONOMIC MOBILITY ACROSS GENERATIONS 6 (2012), https://www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2012/pursuingamericandreampdf.pdf [https://perma.cc/DH6M-ERVZ].

384. JESSICA SEMEGA ET AL., INCOME AND POVERTY IN THE UNITED STATES: 2018, at 12 (2019), https://www.census.gov/content/dam/Census/library/publications/2019/demo/p60-266.pdf [https://perma.cc/F8RZ-QWGH].

385. *See* ICELAND, *supra* note 43, at 56 ("[A] third of all people were near poor and poor."); *Poverty Facts: The Population of Poverty USA*, POVERTY USA (2019), https://www.povertyusa.org/facts [https://perma.cc/VBK9-7XR7] ("And 29.9% of the population—or 93.6 million—live close to poverty, with incomes less than two times that of their poverty thresholds."); Arloc Sherman & Paul N. Van de Water, *Reducing Cost-of-Living Adjustment Would Make Poverty Line a Less Accurate Measure of Basic Needs*, CTR. ON BUDGET & POL'Y PRIORITIES (June 11, 2019), https://www.cbpp.org/research/poverty-and-inequality/reducing-cost-of-living-adjustment-would-make-poverty-line-a-less [https://perma.cc/67TV-7JJS] ("[O]fficial estimates of minimum living costs consistently exceed the poverty line by a wide margin").

386. Taylor Telford, *Income Inequality in America Is the Highest It's Been Since Census Bureau Started Tracking It, Data Shows*, WASH. POST (Sept. 26, 2019), https://www.washingtonpost.com/business/2019/09/26/income-inequality-america-highest-its-been-since-census-started-tracking-it-data-show/ [https://perma.cc/VS6P-F7W8].

387. Chad Stone et al., *A Guide to Statistics on Historical Trends in Income Inequality*, CTR. ON BUDGET & POL'Y PRIORITIES (Jan. 13, 2020), https://www.cbpp.org/research/poverty-and-

while wage stagnation plagues middle class and low-wage workers despite their productivity and low rates of unemployment.[388]

Unrestrained automated profiling risks further entrenching these trends because it can perpetuate inaccurate and biased inferences about people without their knowledge or avenues for recourse, which, in turn, limits opportunities and traps people in cycles of disadvantage.[389] Further, employers and businesses can mine data to adopt practices that limit people's autonomy and chances for economic advancement.[390] In all these ways, automated profiling can lead to digital discrimination and economic exploitation, while masking inaccuracies and incomplete data. Moreover, without a human in the loop, surveillance determinations might punish certain categories of people without due process. Limitations on automated profiling could temper these outcomes. It would push entities relying upon algorithms to provide basic due process protections to impacted individuals, thereby fulfilling values of transparency and accountability, while improving accuracy in decision-making.

C. Right To Be Forgotten and Criminal Records

The GDPR contains a right to be forgotten, guaranteeing data subjects the right to demand that a data controller erase their personal data.[391] The right derives from a 2014 case decided by the European Court of Justice, called *Google v. Spain*, holding that Europeans have a right to demand that search engines remove links to their personal data.[392] In that case, a Spanish national objected to the results of internet searches of his name that brought up evidence of past debt.[393] The court reasoned that a private person's right to privacy overrode Google's economic interests, as well as the general public's

---

inequality/a-guide-to-statistics-on-historical-trends-in-income-inequality [https://perma.cc/QLT3-KUPF].

388. ELISE GOULD, STATE OF WORKING AMERICA: WAGES 2018, at 1 (2019), https://www.epi.org/files/pdf/161043.pdf [https://perma.cc/JGA2-LNAT].

389. Stephen Buranyi, *Rise of the Racist Robots—How AI Is Learning All Our Worst Impulses*, GUARDIAN (Aug. 8, 2017), https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses [https://perma.cc/38SZ-SY3A].

390. Nathan Newman, *How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population*, 18 J. INTERNET L. 11, 12 (2014).

391. GDPR, *supra* note 1, at art. 17.

392. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R. ¶ 97.

393. He also challenged the publication of his debt in a newspaper; however, the Spanish data protection agency rejected that claim, ruling that the newspaper lawfully published that content. That aspect of the decision was not appealed to the European Court of Justice. *Id.* at ¶ 14.

interest in finding the information, although these competing factors require a case-by-case balancing.[394] This right does not delete online content about a data subject altogether; rather, it makes that content more difficult to find via a search engine.[395] A similar, narrowly tailored right to be forgotten in the United States could promote economic justice.

As Dan Solove has noted, "People grow and change, and disclosures of information from their past can inhibit their ability to reform their behavior, to have a second chance, or to alter their life's direction."[396] A second chance can be particularly important for people who experience poverty, which operates as a social stigma. Moreover, "due to modern digital technologies and global networks, forgetting has become the exception, and remembering the new rule."[397] As noted above, the official poverty rate is almost twelve percent.[398] However, poverty in America is not a static condition. Most poor people remain under the poverty line only for short periods of time, although they may cycle in and out of poverty over their lifetimes.[399] Almost half of poverty spells end within a year, while seventy percent end within three years.[400] Only twelve percent of poverty spells last more than a decade.[401] Poverty may be short-term, but it is widespread. Almost half of Americans will fall below the poverty line for at least one year between the ages of twenty-five and seventy-five.[402] At some point, two-thirds of all Americans between twenty and sixty-five will turn to a social welfare program such as food stamps or Medicaid.[403] In short, there is a lot of movement in and out of poverty, largely due to economic instability such as job losses, low wages, caretaking obligations, divorce, and illness.[404] Moreover, poverty is more

394. *Id.* at ¶ 97.

395. Rustad & Koenig, *supra* note 10, at 406.

396. Solove, *supra* note 224, at 533.

397. Michal Lavi, *The Good, the Bad, and the Ugly Behavior*, 40 CARDOZO L. REV. 2597, 2628 (2019).

398. SEMEGA ET AL., *supra* note 384, at 1.

399. ICELAND, *supra* note 43, at 61.

400. *See id.*

401. *Id.*

402. Approximately forty-two percent of Americans will fall into the bottom tenth percentile of the income distribution, while sixty percent will fall into the bottom twentieth percentile for at least one year between the ages of twenty-five and sixty. MARK R. RANK & THOMAS A. HIRSCHL, THE LIKELIHOOD OF EXPERIENCING RELATIVE POVERTY OVER THE LIFE COURSE 1 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4511740/pdf/pone.0133513.pdf [https://perma.cc/YM5T-3NDL].

403. Mark R. Rank, *Rethinking American Poverty*, 10 CONTEXTS 16, 18 (2011).

404. ANN HUFF STEVENS, TRANSITIONS INTO AND OUT OF POVERTY IN THE UNITED STATES 1 (2013), https://poverty.ucdavis.edu/sites/main/files/file-attachments/policy_brief_stevens_poverty_transitions_1.pdf [https://perma.cc/8YBH-6683].

than a low income—it is "better understood as something akin to correlated adversity that cuts across multiple dimensions (material, social, bodily, psychological) and institutions (schools, neighborhoods, prisons)."[405] Algorithms impact all these dimensions, and are used by—or targeted at—all these institutions.

Poor people in America face discrimination due to their economic status, which is compounded by intersectional factors such as race, ethnicity, and gender.[406] Nevertheless, poverty is not a protected class in American anti-discrimination law, meaning that it is perfectly legal to discriminate against poor people.[407] In American culture, poor people are stigmatized as lazy and dishonest and blamed for their economic status, even though poverty is rooted in structural, rather than cultural, factors.[408] Poverty today is driven by a multitude of interlocking factors, including the growth of low-wage jobs; declining power of unions; lack of universal child care, health care, and affordable housing; inadequate education; limited social supports; growing income inequality; and discrimination—in sum, "a failure of the economic and political structures to provide enough decent opportunities and supports for the whole of society."[409]

Danieli Evans Peterman highlights a range of discriminatory practices based on socioeconomic status, writing,

> Employers screen applicants by residential address and weed out people who live in notoriously poor neighborhoods. Municipalities enact zoning rules for the purpose of excluding low income residents. Schools place wealthier students in more advanced classes with more experienced teachers. States require voters to show identification documents that poor people have more difficulty obtaining.[410]

Technology can make each of these forms of poverty discrimination even easier. Employers can use screening services to weed out low-income people from the pool of job applicants. Credit scoring algorithms can lead banks to deny loans to low-income people, thereby entrenching zoning disparities. Public school placement algorithms can favor technologically sophisticated and wealthy parents. Algorithms can be used to gerrymander districts in ways that dilute votes of poor people and people of color.

---

405. Desmond & Western, *supra* note 15, at 308.
406. *See* ICELAND, *supra* note 43, at 107–20.
407. Peterman, *supra* note 74, at 1286–87.
408. ICELAND, *supra* note 43, at 125–30.
409. Rank, *supra* note 403, at 19.
410. Peterman, *supra* note 74, at 1286.

Furthermore, social media is feeding adverse stereotypes about poor people to the gatekeepers of important social resources, such as employers and loan companies. While wealthier people can hire reputation management services to clean up their online profiles, poor people are left with a "tarnished mark" that "undermines their economic and educational opportunities and reinforces social gaps."[411] Thomas Koenig and Michael Rustad identify various "[d]igital marks of shame,"[412] such as obesity and tobacco use that are strongly correlated with poverty but that previously might have remained invisible to these gatekeepers and the general public.[413] Today, these are traits that employers are tracking through applicant screening services, wellness programs, and other surveillance technologies. As a result, employers may be tempted not to hire, or to fire, certain low-income workers to save on health insurance costs. Further, people face inferences not only from their own social media posts but also from data gleaned from their social media "friends," which feeds into their digital profiles.[414] Their friends' habits and preferences are used to make predictions about their conduct. For all these reasons, a right to be forgotten could help low-income people move past negative inferences generated from their economic status.

In the United States, we punish the poor, but we also share certain cultural norms about starting anew that are associated with "the immigrant, pioneer histories of so many Americans" and our individualistic ethos.[415] We see these norms reflected in various settings. For instance, in the justice system, character evidence is generally inadmissible in trials because of a bedrock legal principle that people should be judged by their actions and not their past conduct or personality traits.[416] We also provide people with fresh economic starts through bankruptcy, which allows people and companies to eliminate their debts and begin again with a clean slate.[417] To bolster this financial fresh start, credit reporting agencies cannot include data about bankruptcies after seven to ten years (depending on the form of bankruptcy filed),[418] and employers cannot discriminate against employees who have declared

411. Lavi, *supra* note 397, at 2643.

412. Koenig & Rustad, *supra* note 262, at 596.

413. *Id.* at 600. Obesity rates among the poor are high in part due to the lack of access to fresh food in poor neighborhoods; tobacco rates are higher among the poor due to targeted advertising. *Id.* at 600–01.

414. *Id.* at 611.

415. Jean-Francois Blanchette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 INFO. SOC'Y 33, 35 (2002).

416. FED. R. EVID. 404(b).

417. *See* Blanchette & Johnson, *supra* note 415, at 36.

418. 15 U.S.C. § 1681c(a)(1) (2018).

bankruptcy.[419] FRCA likewise requires erasure of arrests, civil lawsuits, and legal judgments in credit reports after seven years.[420] These measures are designed to limit the stigma associated with bankruptcy and other interactions with the justice system. The United States should follow the lead of the GDPR and expand the right to be forgotten beyond these narrow contexts.

Some commentators contend we should forget about a right to be forgotten in the United States because it is barred by the First Amendment.[421] However, the First Amendment has never been absolute, particularly with regard to private, commercial relationships.[422] For instance, the privacy torts of public disclosure of private facts, invasion of privacy, and defamation do not run afoul of the First Amendment.[423] Similarly, as Neil Richards explains, data privacy laws are constitutional because they pose no "menace [to] a free press,"[424] which is accorded higher levels of protection than private speech. Thus, we have perfectly constitutional laws that aim to keep private our health records and financial information. Frank Pasquale adds that search results are "a matter of algorithmic data processing, not personal (or even corporate) expression," and thus entitled to even less constitutional protection.[425] Any right to be forgotten in the United States will not be a carte blanche right to shape one's internet profile in false or misleading ways, and certainly not to limit or erase reporting by journalists, but it will require balancing the public's interest in information with an individual's right to privacy.

Criminal records are a prime example of why the right to be forgotten is so important to marginalized communities. In America, one-third of the population has a criminal record due to aggressive mass criminalization policies that particularly impact people of color.[426] These records generate

---

419. 11 U.S.C. § 525 (2018). These protections, however, do not apply to private employers' hiring decisions. *See* Shepard, *supra* note 87, at 1751.

420. 15 U.S.C. § 1681c(a)(2).

421. *See, e.g.*, Jeffrey Rosen, *The Right To Be Forgotten*, 64 STAN. L REV. ONLINE 88, 88 (2012), https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ [https://perma.cc/R88S-PH57] (describing the right to be forgotten "as the biggest threat to free speech on the Internet in the coming decade").

422. Lavi, *supra* note 397, at 2645–46. Lavi proposes guidelines for implementing a right to be forgotten in the United States. *Id.* at 2649–73.

423. *See* Rustad & Koenig, *supra* note 10, at 407–08 (discussing the tort for public disclosure of public facts).

424. Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1516 (2015).

425. Frank Pasquale, *Reforming the Law of Reputation*, 47 LOY. U. CHI. L.J. 515, 530 (2015).

426. Jeffrey Selbin, Justin McCrary & Joshua Epstein, *Unmarked? Criminal Record Clearing and Employment Outcomes*, 108 J. CRIM. L. & CRIMINOLOGY 1, 3–4 (2018).

collateral consequences that limit people's access to employment, education, and housing, as well as impact parental rights and freedom of movement—of all which undermine any vision of economic justice.[427] Accordingly, all states have passed expungement laws, which allow people to apply to have certain criminal records either deleted from official public databases or marked as "expunged."[428] These laws are designed to provide people with a "clean slate," so that they can obtain jobs, housing, and other life necessities "which in turn will reduce social and economic hardship for individuals, families, and society."[429]

Expungement laws, however, are undermined by data mining, particularly the buying and selling of personal data for background check purposes. Once a data broker collects a criminal record from a public database, that data lives on in cyberspace.[430] People must play a frustrating game of whack-a-mole, constantly trying to clean up stale data where it emerges. Yet, it can be impossible to know where expunged data is being reported, and even armed with that knowledge, the FCRA process to correct such information in consumer reports is cumbersome and difficult.[431] Moreover, data brokers often evade FCRA's reach.[432] Thus, a right to be forgotten that allows people to demand digital expungements—or that limits release of criminal non-conviction records in the first instance[433]—could enhance our existing expungement laws and expand access to life necessities and economic security for millions of Americans.

Notably, the GDPR treats criminal records as a specially protected class of data, providing that "[p]rocessing of personal data relating to criminal convictions and offences" can happen only under governmental control or laws that ensure safeguards for the rights and freedoms of data subjects.[434] In

---

427. *See* Gabriel J. Chin, *The New Civil Death: Rethinking Punishment in the Era of Mass Conviction*, 160 U. PA. L. REV. 1789, 1790 (2012); Michael Pinard, *Collateral Consequences of Criminal Convictions: Confronting Issues of Race and Dignity*, 85 N.Y.U. L. REV. 457, 489–94 (2010).

428. Selbin et al., *supra* note 426, at 20–22. Expungement laws generally cover arrests that did not result in conviction and misdemeanors.

429. *Id.* at 6.

430. Eldar Haber, *Digital Expungement*, 77 MD. L. REV. 337, 338 (2018) ("The fact that the internet is capable of remembering everything makes expungement statutes ineffective in the digital era.").

431. *Id.* at 355 (describing shortcomings with FCRA remedies).

432. *Id.*

433. *See id.* at 381–83 (advocating for ex ante steps such as keeping non-conviction criminal history records private); Selbin et al., *supra* note 426, at 53 (advocating for automatic record clearing for not guilty verdicts and dismissals of charges).

434. GDPR, *supra* note 1, at art. 10.

the EU, it is not necessary to talk about digital criminal records expungement because criminal records and defendants' identities are kept under wraps by courts in the first instance.[435] Convictions for minor offenses and arrests that do not lead to convictions are never entered into the official record.[436] Private databases of criminal records are illegal.[437] Obviously, expungement laws in the United States are not as broad, as we have a historical commitment to open criminal records.[438] Despite this norm, every state has enacted laws to limit the long-term impact of certain criminal records and to give people a fresh start.[439] Thus, a right to be forgotten could help state expungement laws achieve their goals. More broadly, the right to be forgotten could ensure that the social sorting driven by digital profiling does not become a permanent barrier to economic advancement and that data errors and omissions do not become fixed in time to the detriment of individuals.

D. Public Participation

The GDPR requires public input in certain data privacy programs, and similar public participation opportunities should be adopted and expanded in American privacy laws. The GDPR's public participation requirements attach to Data Protection Impact Assessments (DPIAs), which are reports that data controllers must prepare when they process personal data.[440] DPIAs are required whenever automated processing, particularly using new technologies, "is likely to result in a high risk to the rights and freedoms of natural persons."[441] High risk situations include profiling that has significant effects, processing of sensitive categories of personal data (including criminal convictions), and large-scale monitoring of public areas.[442] A DPIA must contain a description of the intended processing and its purposes, the necessity and proportionality of the processing, the risks to the rights and freedoms of data subjects, and steps and safeguards the controller is taking to

435. Haber, *supra* note 430, at 376.

436. *See* James B. Jacobs & Elena Larrauri, *Are Criminal Convictions a Public Matter? The USA and Spain*, 14 PUNISHMENT & SOC'Y 3, 13 (2012). Employers cannot access records, but they can ask a job applicant for a copy of the official record. *See id.* at 6.

437. *See id.* at 12.

438. Haber, *supra* note 430, at 376–79.

439. Jonathan Rosenfeld, *Expungement Laws Across the United States (Criminal Record Removal)*, ROSENFELD INJ. LAW. LLC (Feb. 4, 2019), https://www.rosenfeldinjurylawyers.com/news/expungement-laws/ [https://perma.cc/YR27-CMRH].

440. GDPR, *supra* note 1, at art. 35.

441. *Id.*

442. *Id.*

protect personal data.[443] Significantly for purposes of this discussion, data subjects also have a role in the DPIA process: "Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing . . . ."[444] The A29WP provides that controllers can obtain public views through a variety of means;[445] one consultant suggests "focus groups, user groups, public meetings, consumer panels, town hall meetings, individual interviews, paired interviews, and surveys."[446] The A29WP adds that an entity whose final processing decision differs from the views of data subjects should document its reasoning.[447]

In the United States, debates around comprehensive privacy legislation and proposed federal bills have not contemplated public participation. By contrast, public participation is a long-standing norm in a wide range of other United States laws,[448] most prominently in environmental regulation, land use, and government programs impacting low income communities.[449] Depending on the statutory regime at issue, participation mechanisms can range from the right to speak at a hearing or submit written comments to more deliberative and collaborative settings, such as small group meetings, information sessions, advisory councils, and consensus-based negotiations.[450]

---

443. *Id.*

444. *Id.*

445. A29WP*, supra* note 336, at 8.

446. *DPIA Under GDPR–Consult Your Data Subjects*, CAPGEMINI (Apr. 23, 2018), https://www.capgemini.com/2018/04/dpia-under-gdpr-consult-your-data-subjects/ [https://perma.cc/TJ7D-RGTD].

447. A29WP, *supra* note 336, at 15.

448. Nancy Roberts, *Public Deliberation in an Age of Direct Citizen Participation*, 34 AM. REV. PUB. ADMIN. 315, 330 (2004) (explaining that public participation is found in areas "such as education, policing, health and social services, justice and environmental systems, and economic and community development").

449. *See, e.g.*, Anne E. Simon, *Valuing Public Participation*, 25 ECOLOGY L. Q. 757 (1999) (environmental); Alejandro Esteban Camacho, *Mustering the Missing Voices: A Collaborative Model for Fostering Equality, Community Involvement and Adaptive Planning in Land Use Decisions*, 24 STAN. ENVTL. L.J. 3, 36–40 (2005) (land use); Audrey McFarlane, *When Inclusion Leads to Exclusion: The Uncharted Terrain of Community Participation in Economic Development*, 66 BROOK. L. REV. 861 (2001) (land use); Jaime Alison Lee, *Rights at Risk in Privatized Public Housing*, 50 TULSA L. REV. 759, 782–84 (2015) (public housing); Tomiko Brown-Nagin, *The Civil Rights Canon: Above and Below*, 123 YALE L.J. 2698, 2730–34 (2014) (describing the Equal Opportunity Act of 1964 and its mandate for "maximum feasible participation" in community action agencies); Tara J, Melish, *Maximum Feasible Participation of the Poor: New Governance, New Accountability, and a 21st Century War on the Sources of Pov*erty, 13 YALE HUM. RTS. & DEV. L.J. 1 (2010) (same); Wendy A. Bach, *Mobilization and Poverty Law: Searching for Participatory Democracy Amongst the Ashes of the War on Poverty*, 20 VA. J. SOC. POL'Y & L. 96 (2012) (same).

450. *See* Thomas C. Beierle & Jerry Cayford, *Environmental Decision Making: What Does Public Participation Add?*, 28 ADMIN. & REG. L. NEWS 6 (2003); Archon Fung, *Putting the Public*

Multiple theories of democracy support public participation in policymaking. To begin with, decision-making is arguably improved when it includes the perspectives of people most impacted, who can provide needed information and novel problem-solving ideas.[451] In technical and scientific realms, public participation can infuse a values-oriented perspective into decision-making that might otherwise be overshadowed by technocratic approaches.[452] Public participation is also touted as a way to build legitimacy in regulatory regimes because people gain trust from processes they understand and shape.[453] A separate strand of participatory democracy theory focuses on benefits to impacted communities as they gain political and social skills though participation in civic life, along with enhanced dignity and self-respect.[454] At bottom, public participation is "anchored by the democratic values of political equality and popular sovereignty which are thrust upon the republican form of government."[455]

Privacy shares similarities with both the environmental and anti-poverty realms. As with the environment, data privacy involves tensions between corporate objectives and the public interest, with oversight by government actors who are subject to regulatory capture. Like natural resources, privacy is an integral resource for human flourishing—but once stripped, it is difficult, if not impossible, to regain.[456] Moreover, the looming dangers of climate change and surveillance capitalism are similarly profound. As with social welfare programs, marginalized communities are uniquely and

---

Back into Governance: The Challenges of Citizen Participation and Its Future, 75 PUB. ADMIN. REV. 513, 517 (2015) (discussing emerging forms, such as multisectoral problem solving and individualized engagement models of participation); Roberts, *supra* note 448, at 331–32 (discussing various mechanisms of citizen participation).

451. *See* Judith E. Innes & David E. Booher, *Reframing Public Participation: Strategies for the 21st Century*, 5 PLAN. THEORY & PRAC. 419, 428–29 (2004); Roberts, *supra* note 448, at 324.

452. Beierle & Cayford, *supra* note 450, at 14.

453. *See* Roberts, *supra* note 448, at 323.

454. *See* Angela M. Gius, *Dignifying Participation*, 42 N.Y.U. REV. L. & SOC. CHANGE 45, 61–62 (2018); McFarlane, *supra* note 449, at 911; Roberts, *supra* note 448, at 323.

455. RAJENDRA RAMLOGAN, SUSTAINABLE DEVELOPMENT: TOWARDS A JUDICIAL INTERPRETATION 165 (2011); *see also* Barbara Bezdek, *Citizen Engagement in the Shrinking City: Toward Development Justice in an Era of Growing Inequality*, 33 ST. LOUIS U. PUB. L. REV. 3, 9 (2013); Fung, *supra* note 450, at 515 (discussing the democratic governance justification for public participation).

456. A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1715 (2015) ("Much like global warming, drift-net data collection and collation creates widespread harms substantially caused by actions not visible to most of those affected."). Froomkin advocates for privacy impact notices, similar to Environmental Impact Assessments, for proposed public or private mass surveillance programs.

harmfully impacted. Yet with regard to data privacy, public involvement is not formally part of existing or proposed regulatory schemes. This may be in part due to public ignorance over the scope and scale of how technology breaches privacy. One international privacy advocacy group reports

> [m]ost consumers still think about online privacy as being primarily concerned with the data they share, and not the data that is observed from their behaviour, inferred or predicted. It is our experience that the general understanding of how profiling works and the kinds of information it can reveal is exceptionally low.[457]

When privacy scandals have come to light, the public has participated primarily through cycles of media-generated outrage, litigation over data security breaches, and particularly for low-income communities, through small-scale public protests. These are not formalized mechanisms for ex ante involvement, but rather, post hoc responses to moments of crisis—which could possibly be avoided through participatory mechanisms in data privacy regimes.

The GDPR's public participation requirement is a modest one, and its "when appropriate" caveat is undefined. Nevertheless, it opens the door to thinking about how more expansive public participation norms might work to enhance American data privacy. To begin with, perspectives of multiple stakeholders should be involved in legislative hearings on data privacy, as well as behind-the-door meetings and negotiations. To date, most testimony, and presumably most lobbying efforts, have been provided by industry representatives, with a small sampling of consumer-oriented, non-profit groups involved. Elected representatives should invite—and consumer, civil rights, and human rights groups should demand—a variety of perspectives in the lawmaking process.

Shaping the laws is a start, but public participation should also be incorporated into ongoing data privacy and data security regimes. As agencies craft regulations, the public comment process should actively seek input from a range of stakeholders, rather than passively waiting for comments to be filed. The California Consumer Privacy Act specifically calls upon the California Attorney General to solicit broad public participation to adopt regulations to "further the purposes of this title," as well as to see if any substantive exceptions and modifications are needed

---

457. *Data Is Power: Profiling and Automated Decision-Making in GDPR*, PRIVACY INT'L 12 (2017), https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf [https://perma.cc/9JKV-SDJC].

to accommodate changing technologies and other laws.[458] This approach should be adopted nationwide. It calls for government outreach, rather than passive receipt of public comment, which is the bare minimum required for regulatory rulemaking in the United States.

Laws and regulations are a start for public participation, but not the end.[459] At a minimum, similar to the GDPR, the United States should require entities that process personal data—both private and governmental—to draft and publish impact assessments that reflect input from a variety of stakeholders.[460] Impact assessments are a regular feature of environmental law, which requires government agencies to prepare a detailed assessment of the impact of proposed projects, including an analysis of whether certain groups will face disproportionate negative consequences.[461] Privacy impact assessments are required by the E-Government Act of 2002 for federal agencies when implementing technology that collects information from the public.[462] However, they do not require public participation in the drafting or post-publication process, and perhaps in part for that reason, the impact of these impact statements has been limited.[463]

In addition, the FTC and other government agencies at the federal and state levels overseeing privacy law implementation should conduct regular

---

458. CAL. CIV. CODE § 1798.185 (West 2020).

459. For a thorough listing and description of multiple participatory mechanisms, see INVOLVE, PEOPLE & PARTICIPATION: HOW TO PUT CITIZENS AT THE HEART OF DECISION-MAKING 56–105 (2005), http://www.sharedpractice.org.uk/Downloads/involve_publication.pdf [https://perma.cc/5RGU-NM5G].

460. On how impact assessments can improve algorithmic decision-making, see Andrew Selbst, Madeleine Clare Elish & Mark Latonero, *Accountable Algorithmic Futures*, DATA & SOC'Y POINTS (Apr. 19, 2019), https://points.datasociety.net/building-empirical-research-into-the-future-of-algorithmic-accountability-act-d230183bb826 [https://perma.cc/DXJ8-TTUB]; Selbst, *supra* note 115, at 169–82.

461. Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 113 (2018).

462. E-Government Act of 2002 § 208, 44 U.S.C. § 3602 (2018); *see also* Dep't of Homeland Sec., *E-Government Act of 2002*, JUST. INFO. SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1287 [https://perma.cc/8WQC-ZEWE]. The PIA is an "analysis of how information is handled by federal agencies," and it must contain a description of the information collected and its purpose, the agency's intended use, whether and with whom the information will be shared, how the information is secured, and whether the privacy policy is in a machine-readable format. *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OFF. MGMT. & BUDGET (Sept. 26, 2003), https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html [https://perma.cc/A2LH-V3UN].

463. Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in U.S. Government Agencies*, *in* PRIVACY IMPACT ASSESSMENT 225, 233 (David Wright & Paul De Hert eds., 2012).

surveys and/or focus groups to seek public input on the impacts of data privacy and to identify trends and concerns. Prior public surveys have revealed that low-income people have greater concerns about their data privacy and feel less secure in their ability to manage their data.[464] In addition, privacy enforcement agencies should hold regular public hearings on emerging data privacy issues and include a range of stakeholders. Notably, past hearings at the FTC have generated informative descriptions of data processing activity along with sound (but unadopted) recommendations.[465] Government agencies should create inclusive consumer and employee advisory councils empowered to gather and share information about data privacy practices and impacts. Data privacy agencies should also engage in public education efforts to inform people about the uses and abuses of their data and their data privacy rights and enforcement options.

Technology can be harnessed for both information gathering and educational purposes. The goal should be to engage in an ongoing dialogue with the public to ensure that the promise of big data is fulfilled, while limiting its more harmful impacts. Through dialogue, society may identify certain digital technologies and data practices that should be constrained or eliminated outright. For instance, some privacy experts have advocated to ban facial recognition technology[466] and targeted advertising,[467] and sustained debate from multiple stakeholders might further shape substantive interventions into technological applications that advance economic justice.[468]

---

464. *See supra* notes 17–21 and accompanying text.

465. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/S2LB-U6AC].

466. *See, e.g.*, Woodrow Hartzog & Evan Selinger, *Facial Recognition is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/PFK2-JCBQ]; Max Read, *Why We Should Ban Facial Recognition Technology*, N.Y. MAG. (Jan. 30, 2020), https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html [https://perma.cc/9UGX-WCAA].

467. *See, e.g.*, David Dayen, *Ban Targeted Advertising*, NEW REPUBLIC (Apr. 10, 2018), https://newrepublic.com/article/147887/ban-targeted-advertising-facebook-google [https://perma.cc/CQ87-DH8E]; Gilad Edelman, *Why Don't We Just Ban Targeted Advertising*, WIRED (Mar. 22, 2020), https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/ [https://perma.cc/HJ24-LJHD].

468. There are numerous laws applicable to specific settings, situations, and relationships that could further enhance data privacy and improve economic justice; some of these exist already in certain state and local jurisdictions. Some examples include limitations on the use of tenant screening reports and tenant blacklisting practices; enhanced controls over the data broker

To be sure, there are many barriers to effective public participation that must be addressed to ensure that participation is meaningful, rather than mere window dressing. In the 1960s, Sherry Arnstein developed an influential "ladder of citizen participation,"[469] describing eight levels of participation "with each rung corresponding to the extent of citizen's power in determining the end product."[470] At the bottom levels are non-participatory mechanisms in which officials talk at participants.[471] The ladder then progresses to token levels of participation, such as consultation; here, citizens may be heard, but they lack the power to shape outcomes.[472] At the top three rungs of the ladder, citizens gain power "with increasing degrees of decision making clout."[473] At the very top, there is citizen control, where "have-not citizens" hold a majority of the decision-making seats or even full managerial control.[474] Consistent with the ladder analogy, empirical studies have shown that the public has the greatest impact when processes are collaborative and deliberative, as opposed to one-way communications, such as testifying at a public hearing or submitting a written comment.[475]

Another barrier to effective public participation can be the expertise needed to master complex scientific and technological issues;[476] this has been a long-standing issue with regard to public participation in environmental law. Data privacy involves complex systems such as machine learning and algorithmic operations. Nevertheless, laypeople are certainly able to understand how they are being impacted by technology on a daily basis, and with some education around digital literacy, can appreciate the unseen hand of technological impacts. It is important to recognize the expertise held by the public; the key is providing a forum for technical expertise and lived

---

industry; limitations on the online payday and installment loan industries; algorithmic accountability statutes for automated decision-making by government agencies; expanded consumer protections against coerced debt (debt accrued by abusers in the name of their victims of intimate partner violence); and limitations on employee and student monitoring and surveillance.

469. Sherry R. Arnstein, *A Ladder of Citizen Participation*, 35 J. AM. PLAN. ASS'N 216 (1969).

470. *Id.* at 217. From the bottom to the top, the rungs are manipulation, therapy, informing, consultation, placation, partnership, delegated power, and citizen control. *Id.*

471. *Id.*

472. *Id.*

473. *Id.*

474. *Id.*

475. *See* Beierle & Cayford, *supra* note 450, at 16; Bezdek, *supra* note 455, at 33–36, 50–51; Innes & Booher, *supra* note 451, at 422.

476. Roberts, *supra* note 448, at 325–26, 339.

expertise to be synthesized.[477] Moreover, data scientists are making strides in translating machine learning concepts for non-experts.

Skeptics of public participation also point to the additional costs and time incurred when additional processes are layered onto already complex decision-making schemes.[478] Supporters counter that long-term costs are saved by improved outcomes. Moreover, participation has benefits beyond outcomes, as people gain skills and knowledge through the process of participation. As people understand the value of their personal data and that of their networks, the value of their participation will be heightened. And, as people feel more secure about their data, they may be more likely to be involved in civic engagement in other areas. In an era of increasing social alienation due to technology, it is possible that public participation in securing data privacy may bring people together.

Finally, in any public participation processes, it is essential to understand the pitfalls that are magnified for low-income people, whose "perspectives . . . may be disregarded due to factors such as race, culture, income, and language; a lack of traditional markers of expertise such as educational or professional credentials; and a lack of other resources that provide influence and bargaining advantages."[479] There are risks that superficial participation can generate distrust, while diverting resources from other social justice reform efforts, and even make it hard to contest outcomes that "carry the presumption of community endorsement."[480] Having a voice is meaningless without real power.[481] Moreover, "a cosmetic process invariably favors those already in power."[482] Accordingly, public participation must be sensitive to multi-cultural values[483] and look to best practices to ensure that it does not further marginalize low-income and minority communities. In the realm of the environment, the environmental justice movement to combat environmental racism has led to multiple,

---

477. Gius, *supra* note 454, at 60–61.

478. *See* Roberts, *supra* note 448, at 324, 339.

479. Jaime Alison Lee, *"Can You Hear Me Now?": Making Participatory Governance Work for the Poor*, 7 HARV. L. & POL'Y REV. 405, 414 (2013); *see also* Gius, *supra* note 454 at 83–84; Svitlana Kravchenko, *The Myth of Public Participation in a World of Poverty*, 23 TUL. ENVTL. L.J. 33, 45 (2009); McFarlane, *supra* note 449, at 914–15; Roberts, *supra* note 448, at 326, 337–38 (discussing the dilemma of excluded or oppressed groups).

480. Douglas NeJaime, *When New Governance Fails*, 70 OHIO ST. L.J. 323, 348 (2009).

481. Jaime Alison Lee, *Poverty, Dignity, and Public Housing*, 47 COLUM. HUM. RTS. L. REV. 97, 135 (2015).

482. Lee, *supra* note 479, at 414.

483. *See generally* John C. Duncan, *Multicultural Participation in the Public Hearing Process: Some Theoretical, Pragmatic, and Analeptical Considerations*, 24 COLUM. J. ENVTL. L. 169 (1999).

concrete participatory best practices to include and empower marginalized populations. These experiences demonstrate that meaningful participation by marginalized groups requires a commitment of resources and affirmative outreach. People's lives are being shaped by digital profiling and surveillance systems, and in a democracy, they should have a say in how these systems operate.

E. Implementation and Enforcement

The GDPR involves multiple stakeholders in implementation, as part of its "data protection by design" approach, which aims to integrate data protection into processing technology, from the design stage and beyond.[484] The GDPR considers privacy as a human right, thereby granting individuals certain (non-absolute) rights, such as the right to explanation and the right to be forgotten, as discussed previously in this Article.[485] Individuals can demand their rights directly from controllers, and in cases of noncompliance, they can file a complaint with their country's Data Protection Authority (DPA) or go to court and seek compensation.[486] Individuals do not shoulder the bulk of privacy enforcement. Rather, the GDPR includes a range of actors to foster compliance. It is a "collaborative governance" regime, which harnesses individual, business, and governmental oversight.[487] Thus, third parties, such as interest groups and digital rights foundations, can litigate on individuals' behalf,[488] and in certain countries, bring cases as representatives of the public interest.[489]

For their part, data controllers must abide by a variety of proactive accountability mechanisms. The GDPR recognizes "that a regulator cannot do everything by top-down control, but that controllers must themselves be involved in the design of less privacy-invasive systems." [490] Among their obligations, controllers need to adopt and implement data protection

484. GDPR, *supra* note 1, at art. 25.

485. *See supra* notes 307–319 and accompanying text.

486. GDPR *supra* note 1, at arts. 77 (right to lodge a complaint with a supervisory authority), 78 (right to an effective judicial remedy against a supervisory authority), 79 (right to an effective judicial remedy against a controller or processor), 82 (right to compensation and liability).

487. *See generally* Margot Kaminski, *Binary Governance; Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (2019).

488. GDPR, *supra* note 1, at art. 80(1).

489. *Id.* at art. 80(2).

490. Edwards & Veale, *supra* note 331, at 50.

policies[491] and security measures and appoint an independent Data Protection Officer to oversee compliance.[492] They must communicate in a timely, concise and intelligible way with data subjects about the processing of their personal data.[493] They must report data breaches to their country's Data Protection Authority, as well as to impacted individuals.[494] They are responsible for GDPR violations committed by their processors, such as data centers and cloud providers.[495] They must draft and carry out DPIAs when their processing of personal data is likely to result in high risk to individual interests, and also consult with their country's DPA when those situations arise.[496] The GDPR provides that controllers can demonstrate their compliance through voluntary certification programs; EU member states are expected to issue compliance standards.[497]

Government also has a key role through each member state's DPA.[498] The DPAs have "investigatory," "advisory," and "corrective" powers.[499] They are charged with gathering information, conducting regular audits, advising companies about compliance mechanisms; and creating codes of conduct and approving certification methods.[500] In terms of enforcement, DPAs can investigate individual complaints, halt unlawful processing, and bring legal proceedings against controllers and processors.[501] Moreover, the GDPR contains bite behind its bark—DPAs can impose maximum fines of up to twenty million euros or four percent of global annual turnover for the most

491. GDPR, *supra* note 1, at arts. 24 (responsibility of the controller), 25 (data protection by design and default), 32 (security of processing).

492. *Id.* at arts. 37 (designation of the data protection officer), 38 (position of the data protection officer), 39 (tasks of the data protection officer).

493. *Id.* at art. 12(1).

494. *Id.* at arts. 33 (notification of a personal data breach to the supervisory authority), 34 (communication of a personal data breach to the data subject).

495. *Id.* at art. 24 (responsibility of the controller); *see also id.* at art. 4 (defining processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller").

496. *Id.* at arts. 35 (data protection impact assessment), 36 (prior consultation).

497. *Id.* at arts. 42 (certification), 51 (supervisory authority).

498. *Id.* at art. 51 (supervisory authority). These are called supervisory authorities in the text of the GDPR but are commonly referred to as Data Protection Authorities. *See* Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. REV. 65, 74 (2018).

499. Hoofnagle et al., *supra* note 498, at 95.

500. GDPR, *supra* note 1, at arts. 57 (tasks), 58 (powers).

501. A full list of tasks and powers of supervisory authorities is in Hoofnagle et al., *supra* note 498.

severe transgressions.[502] Proportional penalties "ensure[ ] that even the titans of industry will not be immune from enforcement."[503]

Taken together, this bundle of obligations provides "systematic accountability"[504] that relieves individuals of shouldering the burden of enforcement. The GDPR framework is thus similar to the concept of technological due process, which scholars, including Danielle Citron,[505] Kate Crawford and Jason Schultz,[506] and Frank Pasquale,[507] have proposed to encapsulate U.S. constitutional due process values of transparency, accuracy, accountability, public participation, and fairness within privacy law.[508] These scholars have taken due process norms developed to constrain government decision-making in an analog world and adapted them to both public and private conduct in the digital world.[509] They call for enhancing individual rights by requiring that people obtain meaningful notice and explanations about automated processing.[510] They advocate for improved hearing processes, along with better training for hearing officers about technology.[511] Further, these scholars advocate for extensive government oversight of algorithmic decision-making via regular audits of algorithms for biases, inaccuracies, and other unfair methodologies, ideally through partnerships with neutral, expert third parties.[512]

Importantly, these scholars extend due process beyond the governmental context, where it exists as a matter of United States constitutional law, and into the private realm, which is particularly appropriate given how intertwined governmental and private data collection and processes operate and the extensive powers private tech companies currently wield over citizens.[513] These ideas have been influential. New York City passed a bill to

---

502. GDPR, *supra* note 1, at art. 83.

503. Casey et al., *supra* note 320, at 167.

504. Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations* 3 (Univ. of Colo. Law Sch., Research Paper No. 19-28, 2019), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456224 [https://perma.cc/6KFW-7XJ4].

505. Citron, *supra* note 127.

506. Crawford & Schultz, *supra* note 234, at 121–22.

507. PASQUALE, *supra* note 279; Citron & Pasquale *supra* note 147.

508. Citron & Pasquale, *supra* note 147, at 20; Crawford & Schultz, *supra* note 234, at 127.

509. *See* Citron & Pasquale, *supra* note 147; Crawford & Schultz, *supra* note 234.

510. Citron & Pasquale, *supra* note 147, at 27; Crawford & Schultz, *supra* note 234, at 122–23.

511. Citron, *supra* note 127, at 1305–08; Crawford & Schultz, *supra* note 234, at 125–26.

512. Citron, *supra* note 127, at 1310–11; Citron & Pasquale, *supra* note 147, at 20–21, 25, 26, 28; Crawford & Schultz, *supra* note 234, at 125–26.

513. Citron & Pasquale, *supra* note 147, at 20–26; Crawford & Schultz, *supra* note 234, at 125–27.

improve algorithmic accountability within city agencies;[514] several states have considered similar bills;[515] and a bill has been proposed in Congress to improve accountability through impact assessments and audits.[516] The idea of algorithmic accountability is to ensure that government agencies and businesses self-assess their automated decision systems and obtain external, expert review of their algorithms, while providing individuals with meaningful due process rights to challenge unfair, biased, or otherwise harmful systems. Using GDPR-style enforcement mechanisms—systemic, collaborative, and diffuse—to develop digital due process in the United States is essential to protecting the rights of all Americans, and particularly marginalized groups, who have less voice within the political process and less access to legal resources to enforce their rights.

V. WHAT ABOUT THE CALIFORNIA CONSUMER PRIVACY ACT?

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2019, and it is currently the most robust consumer privacy law in the United States.[517] Along with the GDPR, it is providing impetus for a federal law,[518] and its implementation is being closely watched. The CCPA creates three core rights for consumers: (1) to know what personal information companies collect and share about them; (2) to have personal information deleted upon request; and (3) to opt-out of the sale of personal information.[519] In addition, as with the GDPR, consumers are protected against

514. New York City passed a bill to study how city agencies use algorithms; the effort has had mixed results. *See* AI NOW INST., CONFRONTING BLACK BOXES 11–16 (Rashida Richardson, ed.) (2019), https://ainowinstitute.org/ads-shadowreport-2019.html [https://perma.cc/3U3L-WQAJ]; Colin Lechter, *New York City's Algorithm Task Force Is Fracturing*, VERGE (Apr. 15, 2019), https://www.theverge.com/2019/4/15/18309437/new-york-city-accountability-task-force-law-algorithm-transparency-automation [https://perma.cc/AK68-T5JW].

515. *See* Sigal Samuel, *10 Things We Should All Demand from Big Tech Right Now*, VOX (May 29, 2019), https://www.vox.com/the-highlight/2019/5/22/18273284/ai-algorithmic-bill-of-rights-accountability-transparency-consent-bias [https://perma.cc/A4BL-MTFV] (discussing efforts in Washington and Oregon).

516. Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019); Algorithmic Accountability Act of 2019, S. 1108, 116th Cong. (2019).

517. Chander et al., *supra* note 27, at 1, 3.

518. *Id.* at 25.

519. To facilitate opt-out requests, businesses must provide a "Do Not Sell My Info" link on their website or mobile app. Consumers can opt out of sales to third parties but not out of collection in the first instance (such as by Facebook and Google as a condition of using the service). CAL. CIV. CODE §§ 1798.100(a), 1798.110(a), 1798.115(a) (West 2020); Chander et al., *supra* note 27, at 22.

discrimination for exercising their statutory rights. Importantly, it scoops data brokers into its coverage.[520]

While it enhances consumer control over personal data significantly for California residents, it is narrower than the GDPR, and thus provides less promise for advancing economic justice. Although it contains a broad definition of personal data,[521] the CCPA only applies to certain businesses[522] and does not apply to non-profits or government agencies.[523] Given the regular interaction between poor people and the state, along with the increase in automated decision-making by government agencies, this omission is significant. Moreover, the CCPA does not provide a right of explanation or a right not to be subject to solely automated processing, which create opportunities to identify and constrain digital discrimination and exploitation while heightening algorithmic accuracy.[524] The CCPA does contain a right to deletion,[525] similar to the right to be forgotten, although businesses under the CCPA have broader exceptions from compliance and fewer obligations to constrain downstream users.[526] In terms of enforcement, individuals can only bring private rights of action under the CCPA for data breaches, leaving enforcement of the other data privacy provisions to the Attorney General.[527] The CCPA contains a more concrete commitment to public participation than does the GDPR, requiring the Attorney General to solicit public opinion in crafting regulations,[528] but it does not appear to require ongoing public participation in monitoring implementation as does the GDPR. The primary difference between the GDPR and the CCPA is that the former permits data processing only where expressly allowed, while the latter permits it freely unless expressly forbidden.[529] Thus, to the degree the CCPA is serving as a model for Congress and other states, those jurisdictions would be well served

520. CAL. CIV. CODE § 1798.120 (West 2020); Chander et al., *supra* note 27, at 14.

521. It includes information linked at the household or device level, which is broader than the GDPR. CAL. CIV. CODE § 1798.140(o)(1) (West 2020).

522. The CCPA applies to businesses with gross annual revenues higher than twenty-five million dollars; or more than fifty percent annual revenues from selling consumer personal information; or engaged in purchase or sell of personal information of at least fifty thousand consumers. *Id.* § 1798.140(c).

523. *See id.* Employees will gain full coverage effective January 1, 2021. *Id.* § 1798.145.

524. *See* Chander et al., *supra* note 27, at 20.

525. CAL. CIV. CODE § 1798.105 (West 2020).

526. Chander et al., *supra* note 27, at 17–18.

527. *Id.* at 21.

528. The Attorney General's Office held seven public forums across the state, and it received and considered more than 300 written comments. OFFICE OF THE ATT'Y GEN., CALIFORNIA CONSUMER PRIVACY ACT (CCPA) FACT SHEET 3, https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf [https://perma.cc/7BPG-ATUH].

529. Chander et al., *supra* note 27, at 19.

to also consider those GDPR-style provisions that could particularly assist their low-income residents.

VI. CONCLUSION

Low-income people in the United States face more serious harms from digital profiling than other Americans. Their digital profiles mark them as poor and lessen their ability to rent a house, get a stable job, obtain a car loan, enroll in college, afford health insurance, or receive adequate medical care. Governments are adopting automated decision-making as a gatekeeper to social services, but these algorithms often contain inaccurate interpretations of law and/or rely on erroneous data, leaving qualified people without sorely needed assistance. Surveillance tools, including facial recognition technology, are more heavily concentrated in low-income and minority communities, stripping people of dignity, ensnaring them in the criminal justice and child welfare systems, and undermining their housing stability.

Currently, neither American privacy laws nor anti-discrimination statutes have the teeth to disrupt these digitized patterns of targeting and exclusion that keep people in poverty and destabilize communities. Society pays the resulting financial and destabilizing costs of incarceration, under-employment, ill health, and family instability. Accordingly, as Congress debates comprehensive privacy legislation, it is imperative that the needs and interests of low-income and marginalized communities are part of the discussion and considered in crafting solutions. The GDPR, which governs data privacy in the European Union, provides a template to spur discussions about linking data privacy to economic justice. In the EU, people are entitled to explanations about automated decision-making and recourse to human decision-makers. They have a right to a digital clean slate to open up future economic opportunities. They have some say in the digital regimes that govern them, and they have meaningful and systemic enforcement mechanisms to secure all these rights. These GDPR provisions alone will not eliminate oppression and injustice. However, they provide enhanced transparency and accountability to people impacted by digital technologies, which in turn, can be building blocks for social justice movements and further, substantive reforms. The United States should adopt similar privacy law provisions to advance civil rights and economic justice.