Harvard Journal of Law & Technology
Volume 39, Number 2 Spring 2026

CODE AND CONSEQUENCES: HOW FRAUD DETECTION ALGORITHMS CRIMINALIZE WELFARE

*Michele E. Gilman**

ABSTRACT

This article investigates the growing use of automated fraud detection systems in public benefits programs, focusing on how these technologies have intensified the surveillance and criminalization of low-income individuals. Across the globe, government agencies deploying fraud detection algorithms have wrongfully accused thousands of people of committing fraud, with devastating consequences, including bankruptcy, job loss, and psychological trauma. These algorithmic systems operate as opaque "black boxes," fueled by historical biases against the poor and largely unaccountable to the individuals they affect. Meanwhile, the private vendors that develop the algorithms reap massive profits from unfulfilled promises of efficiency and cost savings.

The article situates these developments within the broader frameworks of surveillance capitalism and the datafied state, arguing that the convergence of corporate data commodification and government automation has created a new digital dystopia in welfare administration. While "real" fraud — committed by organized criminal syndicates — has increased due to the proliferation of unregulated personal data flows, the state's response has disproportionately targeted vulnerable populations. The article contends that existing legal protections, including due process, privacy law, and anti-discrimination laws, are inadequate to address the systemic harms posed by these algorithms. These doctrines were shaped to restrain human actors; they are not sufficient on their own to govern the scope, scale, and opacity of the datafied state. The article thus calls for a fundamental rethinking of algorithmic governance, urging a shift from the prevailing fraud-first presumption

* Venable Professor of Law and Director of the Saul Ewing Civil Advocacy Clinic at the University of Baltimore School of Law; and Affiliate, Data & Society Research Institute. For their helpful feedback, I would like to thank participants at the 2024 Clinical Law Review Workshop at NYU Law School, the 2025 Privacy Law Scholars Conference at UCLA Law School, the 2025 Law & Society Conference Session on Algorithmic (In)Justice, the Public Law Technology Collaborative, the Race, Law & Technology Seminar at the University of Maryland School of Law, and the Utopian and Dystopian Narratives About Technology Seminar at Georgetown University. Special thanks also for their insights to Professors Dan Hatcher, Chaz Arnett, Madalyn Wasilczuk, Niamh Kinchin, Rebecca Delfino, Conrad Johnson, Praveen Kosuri, Jennifer Urban, Alice Marwick, and Jonathan Kerr, as well as Marc Canellas, Sara Geoghegan, William Agnew, Joel Schmidt, John Davisson, David Blanchard, Laura Padin, Ariel Kennan, and Mary Madden.

embedded in automated systems to a support-first model that affirms the dignity and rights of vulnerable populations.

Harvard Journal of Law & Technology
Volume 39, Number 2 Spring 2026

TABLE OF CONTENTS

I. INTRODUCTION

In 2013, Michigan rolled out a new automated system to identify unemployment insurance fraud.[1] Over a two-year period, the MiDAS system, without any human involvement, accused over 40,000 people of committing fraud and demanded the return of "overpayments" with

1. *See* Stephanie Wykstra, *Government's Use of Algorithm Serves Up False Fraud Charges*, UNDARK (June 1, 2020), https://undark.org/2020/06/01/michigan-unemployment-fraud-algorithm [https://perma.cc/N9WC-VZHE].

400 percent penalties.[2] An audit later revealed that ninety-three percent of the accusations were wrong.[3] The consequences to the falsely accused were severe; more than a thousand people declared bankruptcy, marriages fell apart, and people were denied houses and jobs due to their damaged credit scores.[4] Over a decade of litigation and journalistic investigations of the state and the vendors who designed the technology revealed the system's flaws: MiDAS did not distinguish between fraud and innocent mistakes, it was fed incomplete data, its calculations were inaccurate, and its computer-generated notices were designed to make people inadvertently admit to fraud.[5] This debacle was not an outlier. Deployment of inaccurate and discriminatory welfare fraud detection algorithms has devastated lives across the globe.[6] Yet governments continue to spend millions of taxpayer dollars on these systems, lured by vendor claims of efficiency, accuracy, and cost savings.[7]

Welfare fraud is generally defined as the making of intentional misrepresentations or omissions to obtain government benefits to which one is not eligible.[8] Of course, governments are responsible for the integrity of their spending. Yet for decades, politicians have sounded alarms about welfare fraud without empirical evidence to support the inflated rhetoric.[9] Indeed, prior to the pandemic, most "fraud" was the result of honest mistakes in complying with complex regulatory schemes or theft by other system actors such as agency caseworkers.[10] Despite this reality, welfare fraud hyperbole has been effectively

---

2. *Id.*; Alejandro De La Garza, *States' Automated Systems Are Trapping Citizens in Bureaucratic Nightmares With Their Lives on the Line*, Time Mag. (May 28, 2020, at 14:24 ET), https://time.com/5840609/algorithm-unemployment/ [https://perma.cc/2FZ4-G44Q]; *see also* Bauserman v. Unemployment Ins. Agency, 983 N.W.2d 855, 867 (Mich. 2022).

3. Paul Egan, *False Fraud Cases Against Unemployment Claimants May Hit 50,000*, DETROIT FREE PRESS (Jan. 26, 2017, at 18:21 ET), https://www.freep.com/story/news/local/michigan/2017/01/06/wrongly-accused-ui-agency-reviews-31k-more-fraud-cases/96253414/ [https://perma.cc/HV37-GTUG].

4. *See* Wykstra, *supra* note 1.

5. *See infra* notes 50–58 and accompanying text.

6. *See infra* Sections II.B, III.C.

7. *See* VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 7–8 (2017).

8. *See, e.g.*, GOV'T ACCOUNTABILITY OFF., HOW PREVALENT IS FRAUD IN FEDERAL PROGRAMS? WE TAKE A LOOK — FOCUSING ON UNEMPLOYMENT INSURANCE OVERSIGHT (2023), https://www.gao.gov/blog/how-prevalent-fraud-federal-programs-we-take-look-focusing-unemployment-insurance-oversight [https://perma.cc/3SWA-CPB8].

9. *See* KAARYN GUSTAFSON, CHEATING WELFARE: PUBLIC ASSISTANCE AND THE CRIMINALIZATION OF POVERTY 32–47 (2011) (tracing the history of fraud rhetoric in connection with welfare).

Technically, "welfare" refers to the cash assistance program for families called Temporary Assistance to Needy Families ("TANF"). *Id.* at 44. However, the term "welfare" is more often and colloquially used to refer to the entirety of social safety net programs. *Id.* at 1. This article uses the term "welfare" in its broader sense, referring to TANF or its predecessor cash assistance programs by name when specifically addressing those programs.

10. *See infra* Section III.C.

wielded to decrease public support for poverty relief programs and to increase antipathy for people needing support, particularly people of color.[11]

Scholars such as Kaaryn Gustafson,[12] Khiara Bridges,[13] and John Gilliom[14] have explained how this welfare fraud myth justified an extensive surveillance system over poor people, including caseworker searches of the homes of recipients, drug testing, intrusive questioning, and fingerprinting. In turn, these surveillance systems stigmatized and demoralized recipients and fed a racist narrative about the unworthiness and criminality of low-income people of color. In short, people experiencing poverty rarely committed intentional fraud out of greed, but the government presumed they did, and policies were shaped accordingly.

The automation of public benefits programs has shifted this longstanding landscape. Technology has not only increased the incidence and scale of erroneous fraud accusations, but it has also made it far easier for criminals to steal public benefits — a trend that escalated during the pandemic when benefits systems went entirely online, often to outdated legacy IT systems, and understaffed agencies were too overwhelmed to meet intense public demand.[15] For unemployment insurance ("UI") alone, pandemic-era benefits theft has been estimated at between $100 and $135 billion, amounting to eleven percent to fifteen percent of total UI benefits paid out during the pandemic.[16] Criminal syndicates stole people's identities from online data troves, used bots to file claims in multiple states, and created fake government agency websites to lure people into turning over personal information.[17] Today, benefits fraud is not always a racially-motivated myth; it is real — but it is largely committed by organized criminal syndicates taking advantage of the anonymity of the internet and the unregulated, free flow of personal data.[18] Thus, anti-fraud efforts are necessary, but if unchecked, they will lead to expanded fraud detection systems that are

11. *See* EUBANKS, *supra* note 7, at 13 ("We manage the individual poor in order to escape our shared responsibility for eradicating poverty.").

12. *See* GUSTAFSON, *supra* note 9.

13. *See generally* KHIARA BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017) (explaining how the state regulates poor mothers and mothers-to-be through the Medicaid program).

14. *See generally* JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY (2001) (explaining how welfare recipients live under pervasive, coercive state surveillance).

15. *See* Michele E. Gilman, *Me, Myself, and My Digital Double: Extending Sara Greene's Stealing (Identity) From the Poor to the Challenges of Identity Verification*, 106 MINN. L. REV. HEADNOTES 301, 310–12 (2022).

16. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-106696, UNEMPLOYMENT INSURANCE: ESTIMATED AMOUNT OF FRAUD DURING PANDEMIC LIKELY BETWEEN $100 BILLION AND $135 BILLION 17 (2023), https://www.gao.gov/products/gao-23-106696 [https://perma.cc/3F6G-DDUE].

17. *See infra* Section V.D.

18. *See infra* Section V.D.

likely to wrongfully ensnare eligible, needy people at ever-increasing rates while undermining public support for safety net programs.

For these reasons, we must now understand how fraud detection algorithms sit at the intersection of surveillance capitalism[19] (the corporate commodification of personal data for profit), and the datafied state[20] (government use of technology for decision-making and service delivery). Surveillance capitalism and its unregulated flows of personal information makes "real" fraud committed by criminals easier to commit than ever,[21] and governments are spending millions to purchase fraud detection systems from technology consultants and vendors.[22] These companies rely on a blend of government and private data to fuel their algorithms, the bulk of which was scraped and aggregated without people's knowledge or informed consent.[23] Further, marginalized people are more subject to data scraping because they are surveilled more intensely, in part through the public benefits application process and higher rates of policing.[24] The algorithms that detect fraud are black boxes that lack transparency into their data sources or how the data is used to predict fraud.[25] These black boxes in turn undermine accountability because claimants and their advocates cannot meaningfully challenge decisions that are based on such an opaque information asymmetry.[26] In addition, studies reveal that these algorithmic systems are biased against Black, Brown, and other marginalized claimants, wrongfully accusing them of fraud at higher rates.[27] Further, in the

---

19. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE FRONTIER OF POWER front matter (2018) (defining surveillance capitalism as "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales").

20. Jenna Burrell & Ranjit Singh, *Introduction* to KEYWORDS OF THE DATAFIED STATE (Jenna Burell, Ranjit Singh, Patrick Davison eds., 2024), https://datasociety.net/wp-content/uploads/2024/04/Keywords_Introduction_r_Singh_04242024.pdf [https://perma.cc/EJX3-KRB2].

21. Cassandra Cross, *Meeting the Challenges of Fraud in a Digital World*, *in* THE HANDBOOK OF SECURITY (Martin Gill 3d ed. 2022) ("[F]raud is not new. However, technological developments and the internet have significantly changed the nature of fraud offending and victimisation.").

22. *See infra* Section III.

23. *See* Keely Quinlan, *Automated Public-Benefit Fraud Detection Used by States Subject of New FTC Complaint*, STATESCOOP (Jan. 4, 2024), https://statescoop.com/automated-public-benefit-fraud-detection-state-ftc-complaint/ [https://perma.cc/4JD7-ESK6]; *EPIC Screening and Scoring Spotlight: Pondera's Fraud Prediction Algorithms for Public Benefits*, ELEC. PRIV. INFO. CTR., https://epic.org/pondera-surveillance/ [https://perma.cc/8R5H-LRKG]; Jasmine McNealy, *Consent (Still) Won't Save Us*, *in* FEMINIST CYBERLAW 191, 193–95 (Meg Leta Jones & Amanda Levendowski eds. 2024) (discussing the lack of meaningful consent to personal data collection).

24. *See* EUBANKS, *supra* note 7, at 7.

25. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY 3 (2016) (discussing the concept of "black boxes").

26. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1253–54 (2008).

27. *See infra* Section V.A.1.

digital age, accusations of fraud are now permanent data points that can follow people for the rest of their lives, with collateral consequences that limit their housing, job, and other opportunities.[28]

Given that at least thirty percent of the population participates in a social safety net program,[29] these digital dynamics have massive repercussions. Moreover, at some point *all* Americans — not just low-income citizens — are at risk of a false, algorithmically-generated fraud accusation because of their engagement with government programs that screen for fraud. For instance, most people will eventually retire and receive Social Security and Medicare, and all citizens are connected to the tax system. Surveillance tools are often tested on marginalized populations before they are brought to the mainstream.[30] And they are spreading. Under the second Trump Administration, the Department of Government Efficiency ("DOGE") alleged widescale fraud in federal programs, firing workers and replacing them with artificial intelligence ("AI") to detect fraud.[31] Furthermore, a massive fraud scheme in Minnesota that started during the pandemic appears to have taken advantage of automated systems to steal money from food, housing, and other welfare programs.[32] This highly publicized scandal involved "industrial-scale fraud" committed by criminal conspirators.[33] The Trump Administration then used the scandal as justification to freeze public benefits funding in child care and welfare programs in blue states across the nation that had no connection to the crimes.[34] In short, the stakes for Americans across the income spectrum are high.

---

28. *See* Sarah E. Lageson, Elizabeth Webster & Juan R. Sandoval, *Digitizing and Disclosing Personal Data: The Proliferation of State Criminal Records on the Internet*, 46 L. & SOC. INQUIRY 635, 640–42 (2021) (describing the collection and dissemination of criminal records on the internet); 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.").

29. *See* ASST. SEC'Y FOR PLAN. AND EVAL., U.S. DEPT. OF HEALTH & HUM. SERVS., HOW MANY PEOPLE PARTICIPATE IN THE SOCIAL SAFETY NET? (2023) (examining ten safety net programs aimed at people struggling with economic stability).

30. *See* Virginia Eubanks, *Want to Predict the Future of Surveillance? Ask Poor Communities*, AM. PROSPECT (Jan. 15, 2014), https://prospect.org/power/want-predict-future-surveillance-ask-poor-communities/ [https://perma.cc/4NXY-6VV7]; *cf.* Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/ [https://perma.cc/8CA2-MQ4T] (noting that while "technology creep" is real, more privileged Americans will never experience the worst abuses of surveillance).

31. *See* Geoffrey Fowler, *The Truth About DOGE's AI Plans: The Tech Can't Do That*, WASH. POST (Mar. 3, 2025), https://www.washingtonpost.com/technology/2025/03/03/doge-ai-government-automation/ [https://perma.cc/FBP4-R7CG].

32. *See* Calvert Scott, *What to Know About Minnesota's 'Industrial-Scale Fraud' Scandal*, WALL ST. J. (Dec. 19, 2025, at 06:38 ET), https://www.wsj.com/politics/policy/minnesota-fraud-trump-scandal-113f4315 [https://perma.cc/T9CU-PGDN].

33. *Id.*

34. *See* Minho Kim, *Health Dept. Freezes $10 Billion in Funding to 5 Democratic States*, N.Y. TIMES (Jan. 6, 2026), https://www.nytimes.com/2026/01/06/us/politics/child-care-funding-cuts-trump.html [https://perma.cc/EW9B-P3CS].

Yet, existing law is inadequate to protect people falsely accused of benefits fraud or to prevent criminals from committing fraud. Traditionally, hearings, as afforded by due process, are the fora where people can challenge the government's public benefits decisions.[35] While vitally important, these individualized, in-person hearings are not adequate to combat the systemic harms rendered by the scope and scale of automated systems.[36] And hearings are essentially useless when the black box remains closed. Further, due process rights attach only to government decision-making, while private entities are now essentially running fraud detection programs, raising state action questions for the datafied state.[37] In addition, remedies from successful enforcement of due process rights are awarded years after harm is incurred and compounded by the lingering accusation.[38] Due process was shaped to restrain human actors; it is not sufficient on its own to govern the automated state.

Further, bias against marginalized groups is a known problem in algorithmic systems, largely because the data that trains these systems reflects structural and historical patterns of discrimination.[39] Yet American anti-discrimination law will generally only remedy such biased outcomes if they are intentional, which is both harder to prove and less likely in algorithmic systems.[40] Vendor claims of trade secrecy and state ignorance of the systems they procure undermine transparency, a core feature of democracy. At the same time, under surveillance capitalism, America has few laws regulating the massive collection and sale of personal data and almost no effective protections for people whose identity is stolen to falsely obtain public benefits. Accordingly, with the datafied state relying on surveillance capitalism, and operating against the backdrop of both historical surveillance and the punishment of low-income people, we need to reconceptualize governance over fraud detection algorithms.

In its focus on welfare fraud detection algorithms, this article makes several main contributions. To begin with, it builds upon important studies of welfare surveillance by identifying the emerging harms from fraud detection algorithms, a new form of AI-powered surveillance that adds scope and scale to longstanding racialized and anti-poor policies in the welfare state. Virginia Eubanks has written

---

35. Goldberg v. Kelly, 397 U.S. 254, 261 (1970) (establishing a constitutional right to a pre-termination hearing before the government reduces a person's public benefits).

36. *See infra* notes 393–405 and accompanying text (discussing due process challenges to algorithmic accusations of fraud).

37. *See* Kate Crawford & Jason Schultz, *AI Systems as State Actors*, 119 COLUM. L. REV. 1941, 1942 (2019).

38. *See infra* note 77 (listing statuses of litigation).

39. *See* Lisa Herzog, *Algorithmic Bias and Access to Opportunities*, *in* OXFORD HANDBOOK OF DIGITAL ETHICS 413, 415–18 (Carissa Veliz ed., 2021).

40. *See infra* Section V.A.1.

extensively about the ways that "poor and working-class people are targeted by new tools of digital poverty management and face life-threatening consequences as a result."[41] In highlighting the harms of fraud detection algorithms, this article adds to the mounting evidence of automated inequality.

Further, the article adds to data privacy scholarship arguing for greater protections for personal data. Data privacy scholars have long bemoaned the "dead body" problem, or the difficulty of identifying the harms of data privacy deprivations, which in turn makes it hard to convince policymakers and courts of the need for robust data privacy laws.[42] In response, this article identifies concrete harms flowing from our unregulated personal data and proposes needed solutions. The focus on fraud detection algorithms is essential, as they threaten not only to deprive people of needed assistance, but also to brand them permanently with a Scarlet F which further destabilizes their financial security.

The article also describes how the datafied state is absorbing the products and modalities of surveillance capitalism without adequate legal restraint. State outsourcing of fraud detection exacerbates unequal power dynamics between the state and corporations on the one hand and marginalized people on the other. The article provides a legal analysis revealing how this imbalance is allowed to grow and fester.

The article proceeds as follows. Part II describes the new "digital dystopia" in welfare fraud detection. It highlights case studies in the United States, the Netherlands, and Australia, where large-scale collapses of automated welfare fraud systems occurred with striking similarities.

Part III situates algorithmic surveillance within historical practices and explains how politicized and racist claims of welfare fraud have been used to criminalize poverty. It then provides detailed empirical evidence on the scope of welfare fraud, which has always been low, but which has increased in recent years due to unregulated markets in personal data.

Part IV analyzes welfare fraud detection systems through the lens of surveillance capitalism and the datafied state, the combination of which explains the increase in welfare fraud as well as the increase in wrongful fraud accusations. This Part assesses how the shift in public benefits delivery from caseworkers to technology reinforces and expands longstanding dynamics of surveillance and discrimination,

---

41. EUBANKS, *supra* note 7, at 11.

42. Ann Bartow, *A Feeling of Unease about Privacy Law*, 155 U. PA. L. REV. PENNUMBRA 52, 52 (2006) (discussing how some privacy scholarship suffers from "too much doctrine, and not enough dead bodies," where framing "privacy harms in dry, analytical terms" can fail to shows the ways that "privacy violations can negatively impact the lives of living, breathing human beings").

justified by the specter of fraud. The history of racially motivated rhetoric against welfare fraud has been privatized for corporate profit.

Part V analyzes how existing legal remedies are inadequate to restrain the harms generated by the collision between the datafied state and surveillance capitalism. It organizes the analysis by the values of fairness, accountability, and transparency, which undergird the objectives of both computer science and the administrative state. It also assesses the law's failure to secure personal data, which in turn is allowing criminals to prey on public benefits systems.

Finally, Part VI focuses on solutions that incorporate a support-first rather than fraud-first presumption for welfare claimants. This Part highlights the value of dignity, which is an underpinning of the administrative state that has gotten lost in its technological incarnation. Proposals for a support-first approach to fraud detection in public benefits include the elimination of fraud terminology; reduction of administrative burdens in the public benefits eligibility process; adoption of a rules-as-code approach; pre-testing before fraud detection systems are deployed; mandatory data reporting for transparency; substantive standards for AI governance; stakeholder input into system design; and the maintenance of humans in the loop, or human oversight of algorithmic decisions.

II. THE HARMS OF ROBO-ADJUDICATION

In 2019, the United Nations Special Rapporteur on extreme poverty and human rights warned of the "threat of a digital dystopia," explaining that "systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish."[43] As the case studies below reveal, the dystopia is here. Governments around the world have purchased automated fraud detection systems that share similar deficiencies: inaccurate data and faulty coding; lack of explanations to claimants; denial of meaningful opportunities to challenge fraud accusations; a shift in the burden of proof to the accused; and government obfuscation in the face of systemic problems. Some systems have also proved to discriminate against legally protected characteristics such as race, gender, and national origin. The resulting harms to needy individuals have been catastrophic, including financial, emotional, and mental distress. Belatedly held to account, governments have spent billions to compensate victims, and one government even collapsed under the weight of these mistakes. While algorithmic

43. Press Release, World Stumbling Zombie-Like into a Digital Welfare Dystopia, Warns UN Human Rights Expert, U.N. Press Release (Oct. 17, 2019), https://www.ohchr.org/en/press-releases/2019/10/world-stumbling-zombie-digitalwelfare-dystopia-warns-un-human-rights-expert [https://perma.cc/28MT-JP6B].

injustices in fraud detection systems are rife around the globe,[44] this Part examines well-documented case studies of faulty robo-adjudications in Michigan, as well as in the Netherlands and Australia.

A. Michigan and MiDAS

In 2013, the Michigan Unemployment Insurance Agency replaced its thirty-year-old legacy IT system with a new $47 million system called the Michigan Integrated Data Automated System ("MiDAS").[45] Along with the adoption of MiDAS, the agency laid off a third of its staff, including nearly the entire fraud investigation unit.[46] Very quickly after the rollout, legal services offices were deluged with calls from people who were shocked to learn they had been accused of fraud.[47] Between October 2013 and August 2015, the UI agency charged over 40,000 people with fraud and demanded repayments up to four times the original benefits, plus interest.[48] Many claimants faced penalties between $10,000 to $50,000, and some faced penalties greater than $187,000.[49] In just one year, rates of suspected fraud increased

---

44. *See* Amos Toh, *The Algorithms Too Few People Are Talking About*, HUM. RTS. WATCH (Jan. 5, 2024, at 11:40 ET), https://www.hrw.org/news/2024/01/05/algorithms-too-few-people-are-talking-about [https://perma.cc/RYV7-X7NL] (describing algorithmic fraud detection failures in countries including Denmark, France, and Spain). In India, fraud detection algorithms "wrongly tagged slum dwellers as car owners and inflated incomes of poor widows . . . . [which] deprived several thousands of poor of their right to subsidized food," and another fraud detection algorithm "declared several thousands of living people as 'dead'" thus depriving widows and the elderly of their pensions. Kumar Sambhav Shrivastava, *How We Investigated Welfare Algorithms in India* (Part I), PULITZER CTR. (May 30, 2024), https://pulitzercenter.org/how-we-investigated-welfare-algorithms-india-part-i [https://perma.cc/AC3L-K46S] ("When erroneous decisions of algorithms led to wrongful exclusions of the poor, the onus was on the removed beneficiaries to prove to government agencies that they were entitled to the welfare benefits. Even when they did so, officials often favored the decisions of the algorithms.").

45. Ryan Felton, *Criminalizing the Unemployed*, DETROIT METRO TIMES (July 1, 2015), https://www.metrotimes.com/news/criminalizing-the-unemployed-2353533 [https://perma.cc/N5UX-65TJ]; Rachael Kohl, *Automated Stategraft: Faulty Programming and Improper Collections in Michigan's Unemployment Insurance Program*, 2024 WIS. L. REV. 43, 44 (2024).

46. *The Seven-Year Struggle to Hold an Out-of-Control Algorithm to Account*, MARKUP (Oct. 8, 2022, at 8:00 UTC), https://themarkup.org/newsletter/hello-world/the-seven-year-struggle-to-hold-an-out-of-control-algorithm-to-account [https://perma.cc/7JN3-AAK8]; Robert N. Charette, *Michigan's MiDAS Unemployment System: Created Lead, Not Gold*, IEEE SPECTRUM (Jan. 24, 2018), https://spectrum.ieee.org/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold [https://perma.cc/FJU4-FYR5]; Wykstra, *supra* note 1.

47. Charette, *supra* note 46; Felton, *supra* note 45; *see also* Zynda v. Arwood, 175 F. Supp. 3d 791, 805 (E.D. Mich. 2016) ("Since implementation in 2013, Sugar Law [a legal services organization] has received hundreds of calls from claimants involving fraud issues.").

48. *See supra* note 2.

49. Cahoo v. SAS Analytics, 912 F.3d 887, 893–94 (6th Cir. 2019) [hereinafter *Cahoo II*].

five-fold and the penalties collected by the state rose from $3 million annually to $69 million.[50]

To capture the repayments, the government seized state and federal tax refunds and garnished people's wages.[51] Over 11,000 people declared bankruptcy,[52] tolls were placed on marriages, people attempted suicide, and damaged credit and foreclosures led to loss of homes, rendering some people homeless.[53] People reported struggling to obtain employment because of the collateral consequence of having a "fraud" determination appear on their background checks.[54] Some innocent people faced criminal charges.[55] In Michigan, as elsewhere in the United States, claimants accused of benefits fraud generally can face both administrative proceedings (to recoup overpayments and to face disqualification from the program) and criminal proceedings (to punish fraud).[56]

In 2016, an audit conducted by the agency showed that over ninety-three percent of the fraud charges reviewed were in error.[57] How did the system fail so massively? There were multiple problems. To begin with, the system was operating on incomplete and erroneous data caused in part by a failure to accurately convert data from the legacy

---

50. *See* Kohl, *supra* note 45, at 44; Charette, *supra* note 46.

51. *See* MARKUP, *supra* note 46.

52. *Id.*

53. *See* Felton, *supra* note 45; Ted Roelofs, *Broken: The Human Toll of Michigan's Unemployment Fraud Saga*, BRIDGE MICH. (Feb. 7, 2017), https://www.bridgemi.com/michigan-government/broken-human-toll-michigans-unemployment-fraud-saga [https://perma.cc/B4VL-PLUG].

54. *See* MARKUP, *supra* note 46; Wykstra, *supra* note 1.

55. *See* Felton, *supra* note 45.

56. For administrative charges, impoverished recipients are not entitled to an attorney, and yet an administrative finding of fraud can be used against them in a criminal case. *See* PARKER GILKESSON, CTR. FOR L. & SOC. POL'Y, SNAP "PROGRAM INTEGRITY": HOW RACIALIZED FRAUD PROVISIONS CRIMINALIZE HUNGER 9 (2022). Threats of criminal prosecution are used in some benefits systems to coerce claimants into "admitting fault and accepting the civil consequences without any due process, administrative hearing, criminal process, or legal representation." *Id.*

There can also be adverse immigration consequences to a fraud accusation. *See* LISA NEWSTROM & ANN BLOCK, IMMIGRANT LEGAL RES. CTR., NO CRIME TO BE POOR: DEFENDING WELFARE FRAUD ALLEGATIONS IN CRIMINAL, ADMINISTRATIVE, AND IMMIGRATION PROCEEDINGS, 4 (2023).

57. *See Cahoo II*, 912 F.3d at 894 ("[MiDAS] was deeply flawed; the Michigan Auditor General reviewed over 22,000 of MiDAS' fraud determinations and found that 93 percent of them did not actually involve fraud. In other words, 93 percent of MiDAS' fraud adjudications were false-positives."); Paul Egan, *Suit Filed Against State Fraud Detection Vendor*, DETROIT FREE PRESS (Mar. 2, 2017, at 17:04 ET), https://www.freep.com/story/news/local/michigan/2017/03/02/suit-filed-against-state-fraud-detection-vendor/98646934/ [https://perma.cc/QWS5-XWEE]; Darren Cunningham, *Michigan Reverses 44,000 Jobless Fraud Cases, Refunds $21M*, FOX17 NEWS (Aug. 11, 2017, at 14:18 ET), https://www.fox17online.com/2017/08/11/michigan-reverses-70-percent-of-fraud-cases-to-refund-21m [https://perma.cc/5SWP-2MKG].

system to MiDAS.[58] At the same time, MiDAS did not incorporate data from more recently submitted paper documents.[59] Moreover, MiDAS was programmed to average a claimant's weekly income based on their overall quarterly earnings, yet this formula did not capture weeks in which a claimant did not work.[60] As a result, claimants who honestly reported a lack of earnings in a given week were identified as committing fraud.

In addition, the system's design essentially made claimants inadvertently admit to fraud. When it identified a discrepancy, MiDAS posted a questionnaire to a claimant's online portal, giving them ten days to respond.[61] Yet many claimants' online accounts were dormant given that MiDAS was searching for discrepancies over the prior six years, and people who were no longer claiming UI benefits had no reason to check their accounts.[62] The agency sent no emails, regular mail, or phone calls telling people to check their portal.[63] When a claimant failed to respond or answered yes to one of the questions, "MiDAS robo-adjudicated the fraud issue and automatically determined that the claimant" had committed fraud.[64] From October 2013 to August 2015, the state made no attempt to "consider the facts or circumstances of a particular case, or determine whether the alleged fraud was intentional, negligent, or simply accidental."[65] During this time period, claimants had no opportunity to present evidence or rebut the charges — "no human being took part in this process."[66]

Once MiDAS made a fraud determination, the right to benefits terminated immediately and penalties kicked in.[67] At this point, the agency automatically sent letters to claimants, demanding repayments without ever setting forth the factual basis of the determination.[68] The agency "often" sent the letters to the wrong address or failed to send them at all. A claimant could appeal the determination within thirty days, but "the vast majority" never learned of the determination "until the window to appeal had expired and they had been assessed thousands

58. Paul Egan, *Data Glitch was Apparent Factor in False Fraud Charges Against Jobless Claimants*, DETROIT FREE PRESS (July 30, 2017 at 12:01 ET), https://www.freep.com/story/news/local/michigan/2017/07/30/fraud-charges-unemployment-jobless-claimants/516332001/ [https://perma.cc/AS93-ZQSZ].

59. *Id.*

60. *Cahoo II*, 912 F.3d at 892–93.

61. *Id.* at 893.

62. *Id.*

63. *Id.*

64. *Id.* (quoting Complaint).

65. *Id.* at 894.

66. *Id.*

67. *Id.* at 893.

68. *Id.* at 894.

of dollars in fines."[69] Meanwhile, the agency never answered over ninety percent of calls to its help line.[70]

Administrative law judges who heard cases from claimants who survived this gauntlet repeatedly expressed their frustration with the MiDAS system.[71] One judge reviewing a case stated, "[T]he agency's evidence would be laughable, were it not such a serious matter."[72] By 2014, these accumulating cases were more than enough to alert the agency to its failings, and yet it dug in its heels.[73] Michigan did not halt the automated fraud determinations until 2015, under pressure from the federal government, the filing of a federal class action, intense media attention, and public outcry.[74] In 2017, the legislature passed a law requiring human involvement in fraud determinations and refunded $20.8 million to some residents wrongfully accused of fraud.[75] The state also dropped criminal charges it had filed against 186 people accused of fraud.[76] Meanwhile, numerous lawsuits against the agency, its officials, and the private vendors who designed MiDAS worked through the legal system for over a decade, and some cases eventually resulted in settlements to reimburse certain classes of claimants for wrongfully recouped benefits and penalties.[77]

---

69. *Id.*

70. *Id.*

71. Paul Egan, *Judges Feel Pressured After Blasting Michigan Jobless Agency*, DETROIT FREE PRESS (July 2, 2017, at 07:14 ET), https://www.freep.com/story/news/local/michigan/2017/07/02/judges-michigan-jobless-agency/423502001/ [https://perma.cc/VY2Q-X9L6] (reporting that "managers at the Michigan Unemployment Insurance Agency complained repeatedly to a top official of the Michigan Administrative Hearing System, who in turn, pressured administrative law judges who were too critical of" MiDAS).

72. Egan, *supra* note 58.

73. *See* Charette, *supra* note 46.

74. *Id.*

75. *See* MARKUP, *supra* note 46.

76. *See* Cunningham, *supra* note 57.

77. *See* Zynda v. Arwood, 175 F. Supp. 3d 791 (E.D. Mich. 2016) (alleging various constitutional and federal statutory violations caused by MiDAS fraud determinations against individual defendants in their official capacities); Bauserman v. Unemployment Ins. Agency, 983 N.W.2d 855 (Mich. 2022) (bringing claims against the Unemployment Insurance Agency for violations of due process caused by MiDAS fraud determinations); Cahoo v. SAS Institute Inc., 322 F. Supp. 3d 772 (E.D. Mich. 2018) [hereinafter *Cahoo I*] (marking the first decision in a lengthy case history, finding due process claims plausible where UI claimants alleged violations of due process among other claims against three vendors and several individual state agency officials).

In the *Zynda* settlement, the state agreed to stop automated fraud determination and to submit each allegation to human review. Stipulated Order of Dismissal, Maurice and Jane Sugar Law Ctr. for Econ. & Soc. Justice v. Arwood, No. 15-cv-11449 (E.D. Mich. Feb. 2, 2017). However, litigation alleging that the state breached the agreement is ongoing. *See* Danielle Ferguson, *Mich. Residents, Some Claims Cut from Frozen Benefits Case*, LAW360 (Mar. 25, 2025, at 16:34 ET), https://www.law360.com/articles/2315078/mich-residents-some-claims-cut-from-frozen-benefits-case [https://perma.cc/5PRK-GYCT] (alleging that the agency is still improperly freezing UI benefits and seeking repayment).

B. The Netherlands and the Child Benefit Scandal

The Netherlands takes a strict stance on welfare fraud.[78] In 2013, the tax authorities adopted an automated system to identify fraud in the administration of child care benefits.[79] The system used an algorithm that associated a fraud risk with low-income and ethnic minorities, who programmers identified as more likely to commit fraud.[80] As many as 30,000 parents, disproportionately members of those groups, were accused of fraud and forced to repay benefits and fines, often totaling

---

Bauserman, a class action against the state agency took over ten years to litigate, resulted in 2024 in a $20 million settlement to reimburse class members who were wrongfully accused of fraud.

The *Cahoo* lawsuit was brought in 2017 by four plaintiffs against state officials and three private contractors and resulted in a 2024 settlement of $120,000 from one contractor and $60,000 from another. *See* Adrienne Roberts, *Claimants Falsely Accused of Michigan Unemployment Fraud Settle with Vendors for $180K*, DETROIT FREE PRESS (Jan. 24, 2024, at 16:45 ET), https://www.freep.com/story/money/business/michigan/2024/01/24/michigan-unemployment-fraud-lawsuit/72324312007/ [https://perma.cc/6CF9-72FV]. The state officials were ultimately dismissed from the case. Cahoo v. SAS Inst., Inc., 71 F.4th 401 (6th Cir. 2023).

In *Saunders v. State of Michigan UIA*, brought in 2022 on behalf of plaintiffs who had to repay benefits for alleged fraud before resolving their appeals, the parties reached a settlement of $55 million, pending approval as of April 2025, No. 2022-000007, 2025 WL 2832596 (Mich. Ct. Cl., Mar. 3, 2025). *See* Jon King, *$55 Million Settlement Against State Unemployment Agency Given Preliminary Approval*, MICH. ADVANCE (Apr. 30, 2024, at 10:43 ET), https://michiganadvance.com/briefs/55m-settlement-against-state-unemployment-agency-given-preliminary-approval/ [https://perma.cc/PVZ5-M333].

Individual cases also continue to percolate through the system. *See, e.g.*, Scott v. Dept. of Labor & Econ. Opp., 2023 WL 3671021 (Ct. App. Mich. 2023) (addressing timeliness of appeal of fraud determination under MiDAS).

78. Matt Burgess, Evaline Schot & Gabriel Geiger, *This Algorithm Could Ruin Your Life*, WIRED (Mar. 6, 2023, at 07:00 ET), https://www.wired.com/story/welfare-algorithms-discrimination/ [https://perma.cc/PY4G-BZVW]; AMNESTY INT'L, XENOPHOBIC MACHINES: DISCRIMINATION THROUGH UNREGULATED USE OF ALGORITHMS IN THE DUTCH CHILDCARE BENEFITS SCANDAL 5 (2021), https://www.amnesty.org/en/documents/eur35/4686/2021/en/ [https://perma.cc/2K97-FHMG].

79. Kevyn Levie, *The Dutch Government's Benefits Scandal is Rooted in Stigma Against Welfare Recipients*, JACOBIN (Jan. 23, 2021), https://jacobin.com/2021/01/dutch-welfare-benefits-childcare-scandal [https://perma.cc/7N37-6Q6Q] (explaining that in the Netherlands, parents are eligible for a state contribution toward the costs of day care, which can be up to ninety percent of the actual costs for low-income households).

80. Melissa Heikkila, *Dutch Scandal Serves as a Warning for Europe Over Risks of Using Algorithms*, POLITICO (Mar. 29, 2022, at 18:14 CET), https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/ [https://perma.cc/4XVF-EBNY] (explaining that the tax authority processed data on the dual nationality of applicants); '*Unparalleled Wrong' was Done to Parents Accused of Childcare Fraud: Report*, DUTCH NEWS (Dec. 17, 2020), https://www.dutchnews.nl/2020/12/unparalleled-wrong-was-done-to-parents-accused-of-childcare-fraud-report/ [https://perma.cc/CK87-2VE9] (explaining that "dual nationality" was a data point linked with likelihood of committing fraud); *Dutch Childcare Allowance Scandal: The Importance of Investigation Powers*, EQUINET (Nov. 3, 2022), https://equineteurope.org/netherlands-institute-for-human-rights-role-in-the-investigation-of-the-childcare-allowance-scandal/ [https://perma.cc/427N-V7TU] (explaining that persons of foreign descent were 3.52 times more likely to be identified for fraud).

thousands of euros, which they could not afford.[81] Impacted individuals suffered serious consequences including increased poverty, mental distress, and even suicides,[82] and over 1,600 children were taken into foster care.[83]

At the same time, accused individuals could not uncover the reasons underlying the fraud accusations or what evidence was missing from their applications, yet they had the burden of proving their innocence.[84] Moreover, parents faced lengthy delays in challenging those decisions.[85] The vast majority of the accusations were the result of either administrative mistakes or discriminatory algorithmic targeting.[86] Meanwhile, government officials hid information about the system's operation and misled Parliament and the public. A subsequent parliamentary investigation critiqued "the basic attitude of mistrust, following from the assumption that eighty percent of the recipients were fraudsters."[87] The scandal ultimately lead to the resignation of the Dutch government in January 2021.[88] The government has promised to repay up to 30,000 euros to victims, although this has been delayed

81. *See Childcare Benefit Report Slams Failings Which Ruined Lives*, DUTCH NEWS (Feb. 26, 2024), https://www.dutchnews.nl/2024/02/childcare-benefit-report-slams-failings-which-ruined-lives/ [https://perma.cc/7B95-57X7]; AMNESTY INT'L, XENOPHOBIC MACHINES, *supra* note 78, at 12; Rik Peeters & Arjan C. Widlak, *Administrative Exclusion in the Infrastructure-Level Bureaucracy: The Case of the Dutch Daycare Benefit Scandal*, 83 PUB. ADMIN. REV. 863, 867 (2023).

82. *See* Josien Arts & Marguerite Van Den Berg, *What the Dutch Benefits Scandal and Policy's Focus on "Fraud" Can Teach Us About the Endurance of Empire*, 45 CRIT. SOC. POL'Y 177, 179–80 (2025).

83. *Childcare Benefit Report*, *supra* note 81.

84. *See* Arts & Van Den Berg, *supra* note 82, at 181; Rik Peeters & Arjan C. Widlak, *Administrative Exclusion in the Infrastructure-Level Bureaucracy: The Case of the Dutch Daycare Benefit Scandal*, 83 PUB. ADMIN. REV. 863, 864 (2023).

85. *See* AMNESTY INT'L, *supra* note 78, at 12; Peeters & Widlak, *supra* note 81, at 867.

86. *See* Sofia Ranchordás & Luisa Scarcella, *Automated Government for Vulnerable Citizens: Intermediating Rights*, 30 WM. & MARY BILL RTS. J. 373, 379, 398 (2021). The government was unable to provide evidence of wrongful intent in ninety-four percent of cases. *See* Peeters & Widlak, *supra* note 81, at 863.

87. Menno Fanger & Robin Simonse, *The Implosion of the Dutch Surveillance Welfare State*, 51 SOC. POL'Y & ADMIN. 264, 265 (2023).

88. Jon Henley, *Dutch Government Resigns Over Child Benefits Scandal*, GUARDIAN (Jan. 15, 2021, at 09:32 ET), https://www.theguardian.com/world/2021/jan/15/dutch-government-resigns-over-child-benefits-scandal [https://perma.cc/KTZ4-RDU7]. After his resignation, Prime Minister Mark Rutte remained in charge of the government in a caretaker role and won office again in March 2021, where he served until 2024. See Paul Kirby, *Mark Rutte: Survivor of Dutch Politics in Fight for Political Life*, BBC NEWS (Apr. 2, 2021), https://www.bbc.com/news/world-europe-39289468 [https://perma.cc/5RDS-TTDE] ("The [child benefits] scandal barely figured in the election campaign.").

while victims' personal debts continue to balloon.[89] Moreover, the scandal has not led the Netherlands to reform its digital governance.[90]

C. Australia and Robodebt

In Australia, the robodebt scandal constituted "the Australian government's most catastrophic policy failure in its history."[91] Starting in 2015, the Australian government pledged to crackdown on welfare fraud and initiate billions in cost savings by adopting an automated system to recover overpaid benefits in a variety of social welfare programs.[92] The algorithm used cross-matching of social security payments and past income tax returns to identify discrepancies.[93] However, it relied on a flawed income-averaging algorithm to calculate debts.[94] Between 2016 and 2020, over 526,000 people were accused of fraud via automated debt notices demanding repayment of alleged

89. Morgan Meaker, *The Fraud-Detection Business Has a Dirty Secret*, WIRED (Mar. 7, 2023, at 07:00 ET), https://www.wired.com/story/welfare-fraud-industry/ [https://perma.cc/DA93-3URA] (stating that government compensation is not adequate to cover the debt accrued by impacted families). The Netherlands was also the site of the SyRI scandal, in which the government used a fraud detection system across government agencies that targeted "areas with high proportions of low-income residents, migrants and ethnic minorities," without according these people due process. Naomi Appelman, Ronan Ó. Fathaigh & Joris van Hoboken, *Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands*, 12 J. INTELL. PROP., INFO. TECH. & ELEC. COMMERCE L. 257, 258 (2021) (citation omitted), https://www.jipitec.eu/jipitec/article/view/324/317 [https://perma.cc/DYP2-5CAX]. A Dutch court ultimately ruled that SyRI was unlawful. Marvin van Bekkum & Frederik Zuiderveen Borgesius, *Digital Welfare Fraud Detection and the Dutch SyRI Judgment*, 23 EUR. J. SOC. SEC. 323, 328 (2021). The case is discussed *infra* at text accompanying notes 357–359.

90. *See* Ranchordás & Scarcella, *supra* note 86, at 380.

91. *Unraveling Robodebt: Legal Failures, Impact on Vulnerable Communities and Future Reforms*, UNIV. SYD. NEWS (Dec. 13, 2023), https://www.sydney.edu.au/law/news-and-events/news/2023/12/13/unraveling-robodebt-legal-failures-impacts.html [https://perma.cc/EDD3-PGLG]. It has been called "a crisis, a scandal, a stunning failure of competence, institutional failure and malfeasance, extortionate, negligent, unconscionable, a scandalous example of state dishonesty and collusion, an elaborate shame, a manifestation of venality, incompetence and cowardice and 'a catastrophic, multisystem failure within the Australian Public Service.'" Robert van Krieken, *The Organization of Ignorance: The Australian "Robodebt" Affair, Bureaucracy, Law and Politics*, 50 CRITICAL SOCIO. 1379, 1380 (2024) (citation omitted).

92. Tapani Rinta-Kahila, Ida Someh, Nicole Gillespie, Marta Indulska & Shirley Gregor, *Managing Unintended Consequences of Algorithmic Decision-Making: The Case of Robodebt*, 14 J. INFO. TECH TEACHING CASES 165, 165–66 (2023); Peter Whiteford, *Debt by Design: The Anatomy of a Social Policy Fiasco — Or Was It Something Worse?*, 80 AUSTRALIAN J. PUB. ADMIN. 340, 340–41 (2021).

93. Whiteford, *supra* note 92, at 341.

94. Toby Murray, Marc Cheong, & Jeannie Paterson, *The Flawed Algorithm at the Heart of Robodebt*, PURSUIT (July 10, 2023), https://pursuit.unimelb.edu.au/articles/the-flawed-algorithm-at-the-heart-of-robodebt [https://perma.cc/JP5W-GA7B] ("As anyone who has ever worked a casual job will know, averaging a year's worth of earnings across each fortnight is no way to accurately calculate fortnightly pay. It was this flaw that led the Federal Court to declare in 2019 that debt notices issued under the scheme were not valid."). Previously, there was human review of discrepancies. Whiteford, *supra* note 92.

overpayments, without sufficient evidence or explanation and without human scrutiny.[95] Victims were forced to either repay their benefits or prove their innocence, which shifted the burden of proof from the government to claimants.[96] This was particularly difficult for claimants who lacked internet access or the digital literacy to engage with the online interface.[97] Further, the website was designed in a way that trapped people into inadvertently admitting guilt — a type of dark pattern forcing people toward certain outcomes.[98] It was nearly impossible to reach a human decision-maker.[99]

Many claimants faced extreme financial hardship in making overpayments, feeling "pressured to use options which exacerbated their financial insecurity. Some took out loans, depleted their superannuation, or used credit cards to repay the debts raised against them."[100] Extreme mental distress resulted, including at least three known cases of suicide.[101] Even when the system's failings and cruelty became widely apparent in 2017, the government staunchly defended the system, misled the public, and attacked its critics.[102]

In November 2019, the Australian government finally ended the robodebt scheme after victims challenged it in court,[103] where it was found to be illegal.[104] Subsequently, in May 2020, the government announced it would refund more than 380,000 people who had been wrongly issued debts under the scheme, totaling approximately $1.8 billion in settlement.[105] Including the settlement, the net cost to the government totaled $2.37 billion.[106] A parliamentary investigation of the

---

95. Adam Hannah & Linda Courtenay Botterill, *Avoid the Brakes: Malign Policy and Legal Advice in the Robodebt Scandal*, 44 POL'Y & SOC. 229, 234 (2025), https://academic.oup.com/policyandsociety/article/44/2/229/8246832 [https://perma.cc/72C6-2WLS] ("In total, 526,000 people (roughly one in every 50 Australians) received an illegitimate debt notice between 2016 and 2019.").

96. ROYAL COMMISSION INTO THE ROBODEBT SCHEME, REPORT VOL. 1 at 328, 332 (2023), https://robodebt.royalcommission.gov.au/system/files/2023-09/rrc-accessible-full-report.PDF [https://perma.cc/A3TV-ZTRP]; Whiteford, *supra* note 92, at 341.

97. ROYAL COMMISSION, *supra* note 96, at 329.

98. Donald Moynihan, Morten Hybschmann, Kathryn Gimborys, Scott Loudin & Will McClellan, *Digital Administrative Burdens and Clawback Logics: The Australian Robodebt Scheme*, 8 PERSPS. ON PUB. MGMT. & GOVERNANCE 187, 189–90 (2025) (explaining that people clicked the "next" button on the bottom of screen without realizing it constituted admission of guilt).

99. ROYAL COMMISSION, *supra* note 96, at 328.

100. *Id.* at 332.

101. Frances Mao, *Robodebt, Illegal Australian Welfare Hunt Drove People to Despair*, BBC (July 7, 2023), https://www.bbc.com/news/world-australia-66130105 [https://perma.cc/5GXG-AN74].

102. ROYAL COMMISSION, *supra* note 96, at xxvii ("The government was, the DHS and DSS ministers maintained, acting righteously to recoup taxpayers' money from the undeserving.").

103. Whiteford, *supra* note 92.

104. Rinta-Kahila et al., *supra* note 92, at 168.

105. *Supra* note 98, at 190.

106. *Id.* The scandal contributed to the Liberal Party's loss in 2022 elections. *Id.* at 191.

scandal concluded that "Robodebt was a crude and cruel mechanism, neither fair nor legal, and it made many people feel like criminals."[107] The investigation also found that the government falsely exaggerated incidents of welfare fraud which, in actuality, were "miniscule" or less than 0.1 percent of cases — yet "that is not the impression one would get from what ministers responsible for social security payments have said over the years."

D. Algorithmic Models in Fraud Detection

In each of the failures described above, people suffered serious harms from unfair algorithmic systems lacking transparency and limited accountability. However, the algorithms at issue differed in their models. An algorithm is a set of mathematical instructions that tells a computer how to complete a task.[108] Automated decision-making uses algorithms to simplify complex decisions by dividing a single decision into several discrete tasks performed on digital data.[109] Algorithms range from the very simple, such as running a decision tree, to the very complex.[110] At the more complex level, some algorithms use machine learning — a form of artificial intelligence ("AI") — to analyze large sets of data in order to recognize patterns or make predictions.[111] Algorithmic systems are powerful; they can analyze massive datasets efficiently and consistently.[112] However, as the case studies show, algorithmic systems can also be erroneous and arbitrary, as well as perpetuate embedded biases in datasets against marginalized groups.

In Michigan, by all appearances, the MiDAS fraud detection system was based on a rudimentary rules-based algorithm that compared data from different sources and searched for discrepancies. By contrast, in the Netherlands, the algorithms underlying the child benefits tax system and the since-discredited SyRi algorithm for social welfare had machine learning elements that attempted to predict the type of person more likely to commit fraud based on past data.[113] Predictive algorithms have raised concerns in a variety of contexts. In the child welfare system, some jurisdictions use algorithms to determine which allegations of abuse and neglect to investigate.[114] These algorithms embed

---

107. ROYAL COMMISSION, *supra* note 96, at xxix.

108. *See* HANNAH FRY, HELLO WORLD: HOW TO BE HUMAN IN THE AGE OF THE MACHINE 7–8 (2018).

109. *See id.* at 8.

110. *See id.* at 10–11.

111. *See id.*; Kristin N. Johnson, *Automating the Risk of Bias*, 87 GEO. WASH. L. REV. 1214, 1236–38 (2019); MEREDITH BROUSSARD, MORE THAN A GLITCH: CONFRONTING RACE, GENDER, AND ABILITY BIAS IN TECH 12 (2023).

112. *See* Johnson, *supra* note 111, at 1239; FRY, *supra* note 108, at 198–99.

113. *See* Ranchordás & Scarcella, *supra* note 86, at 398.

114. *See* EUBANKS, *supra* note 7, at 127–73.

racial and class biases 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.[115] 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.[116]

For sentencing and bail determinations, some judicial systems have adopted algorithms designed to predict recidivism.[117] An investigative report by ProPublica 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 underpredicting the risk for White defendants (false negatives).[118] A subsequent study revealed that the algorithm was no better at predicting risk than random people solicited for an online survey.[119]

In these predictive systems, discrimination is baked into the data. As 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] Further, people are not being judged as individuals, but rather, with regard to how they compare to larger groups to which they belong.[121] These presumptions undermine human dignity and autonomy. Fraud detection algorithms are increasingly using machine learning for predictive purposes. While these

---

115. *See id.* at 146–47, 156–57; Sarah Valentine, *Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control*, 46 FORDHAM URB. L.J. 364, 384–85 (2019).

116. *See* Valentine, *supra* note 115, at 380–81.

117. *See* Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043, 1072–76 (2019); 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/2YMX-S4ZX].

118. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminalsentencing [https://perma.cc/ND3T-B68Q]. The creator of COMPAS, a company called Northpointe, defended the algorithm's fairness, and this dispute about the meaning of "fairness" has received wide coverage and analysis. *See, e.g.*, Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218, 2234–37 (2019).

119. Julia Dressel & Hany Farid, *The Accuracy, Fairness, and Limits of Predicting Recidivism*, SCI. ADVANCES 1, 3 (2018).

120. Dorothy E. Roberts, *Digitizing the Carceral State*, 132 HARV. L. REV. 1695, 1708 (2019) (reviewing VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018)).

121. Laurel Eckhouse, Kristian Lum, Cynthia Conti-Cook & Julie Ciccolini, *Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment*, 46 CRIM. JUST. & BEHAV. 185, 198 (2019); *see also* Sofia Ranchordás & Ymre Schuurmans, *Outsourcing the Welfare State: The Role of Private Actors in Welfare Fraud Investigations*, 7 EUR. J. COMPAR. L. & GOVERNANCE 5, 30 (2020) ("Probabilistic models that act on group characteristics rather than a qualitative assessment of an individual's characteristics may contravene the Human Rights Act (in the United Kingdom), the EU Charter of Fundamental Rights, and the ECHR.").

algorithms promise greater accuracy in identifying fraud, recent history shows governments will buy sloppy tools with inadequate oversight.[122]

III. WELFARE SURVEILLANCE AND THE REALITIES OF FRAUD

Historically, rates of intentional fraud in public benefits programs have been lower than the prevailing rhetoric would suggest. Yet governments have used anti-fraud rhetoric to justify extensive surveillance of the poor, which in turn is a form of social control that generates stigma.[123] Welfare surveillance serves the political purposes of "containment of alleged social contagion, evaluation of moral suitability for inclusion in public life and its benefits, and suppression of working people's resistance and collective power."[124] By generating stigma, surveillance decreases public support for poor relief programs and discourages needy people from seeking assistance that could help them meet their basic needs.[125] It also inflicts psychological effects on its targets, including stress, fear, and shame.[126]

Prior to the rise of the datafied state, surveillance of public benefits recipients in the name of fraud prevention included "analog" tactics such as home visits, intrusive questioning by caseworkers, and drug tests. Today, new surveillance tactics operate through technology. They include predictive technologies, location tracking of service recipients, and facial recognition technologies. These methods exponentially magnify the effects of mistakes and biases over vast swaths of the

---

122. *See* Complaint, *In re* Thomson Reuters Corp. (F.T.C. Jan. 3, 2024) (filed by the Electronic Privacy Information Center ("EPIC")), https://epic.org/wp-content/uploads/2024/01/EPIC-FTC-Thomson-Reuters-Complaint.pdf [https://perma.cc/B8ZF-YSJD] [hereinafter EPIC Complaint]. The complaint describes the machine learning aspects of the tool. *See* ¶¶ 42–53; *see also* AMNESTY INT'L, DENMARK: CODED INJUSTICE: SURVEILLANCE AND DISCRIMINATION IN DENMARK'S AUTOMATED WELFARE STATE 8 (2024), https://www.amnesty.org/en/documents/eur18/8709/2024/en/ [https://perma.cc/6VZG-HXVK] ("As of 2019, UDK was reported to be using about 60 different artificial intelligence (AI) and machine learning (ML) models to identify individuals it believed were highly likely to be receiving benefits fraudulently.").

123. *See* GUSTAFSON, *supra* note 9, at 32–37, 51.

124. Virginia Eubanks, *Technologies of Citizenship: Surveillance and Political Learning in the Welfare System*, *in* SURVEILLANCE AND SECURITY: TECHNOLOGICAL POLITICS AND POWER IN EVERYDAY LIFE 89, 90 (Torin Monahan ed., 2006).

125. Jessica Lasky-Fink & Elizabeth Linos, *Improving Delivery of the Social Safety Net: The Role of Stigma* 3 (Harv. Kennedy School, Fac. Rsch. Working Paper Series, No. RWP22-022, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4040234 [https://perma.cc/7MUF-TNFX] ("Yet, despite clear evidence of net benefits for those who participate, 20 to over 50 percent of households do not utilize programs for which they are eligible."); *see also* Rebecca de Souza, *Communication, Carcerality, and Neoliberal Stigma: The Case of Hunger and Food Assistance in the United States*, J. APPLIED COMMC'N. RSCH. 1, 4 (2022) ("Neoliberal stigma operates recursively at individual, interpersonal, and structural levels to reinforce relations of power and maintain the social order.").

126. *See* de Souza, *supra* note 125; GILLIOM, *supra* note 14, at 66–67, 78 (summarizing interviews with welfare recipients in Appalachia in the early 1990s).

population.[127] At the same time, surveillance capitalism, with its unregulated markets in personal data, creates the conditions that give thieves easy opportunities to steal benefits. This Part traces the shift in government assistance programs from analog to digital surveillance and sets forth the available data about welfare fraud, concluding that welfare surveillance criminalizes innocent recipients without any empirical basis for the fraud-first presumption that is coded into surveillance systems.

A. From Home Visit to Algorithmic Surveillance

Poor people in America have always faced state surveillance based on an inherent mistrust of the poor.[128] In the United States, poverty is considered a moral failing, and our individualistic ethos equates a failure to succeed in capitalism with a behavioral choice.[129] When the New Deal created the modern welfare state, surveillance of the "undeserving poor" — able-bodied adults seen as capable of doing work — was a policy centerpiece.[130] As more Black families became eligible for cash assistance in the 1950s and 1960s, some states conducted midnight raids on applicants' homes to ensure single mothers were not living with a man and administered moral fitness tests to determine a home's suitableness for raising children.[131] These tactics aimed to "reduce the

127. *See* Esra Gules-Guctas, *How Do Algorithmic Decision-Making Systems Used in Public Benefits Determinations Fail? Insights from Legal Challenge*s, PUB. ADMIN. REV. 1, 8 (2025), https://onlinelibrary.wiley.com/doi/pdf/10.1111/puar.70043 [https://perma.cc/B56K-4EJY] ("Algorithmic administrative errors (AAEs) are not isolated incidents but systemic, embedded failures. They arise when the translation of statutory requirements into computational logic is compromised by flawed data, problematic design choices, or inherent system limitations.").

128. *See* Mary Madden, Michele Gilman, Karen Levy & Alice Marwick, *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 58–59 (2017) (describing surveillance of the poor from the colonial era through the present).

129. *See* Michele Estrin Gilman, *Expanding Civil Rights to Combat Digital Discrimination on the Basis of Poverty*, 75 SMU L. REV. 571, 585 (2022) (describing the dominant ideology around poverty); *see also* STEPHEN J. MCNAMEE & ROBERT K. MILLER, JR., THE MERITOCRACY MYTH 1–2 (2d ed. 2009); Mark R. Rank, *Toward a New Understanding of American Poverty*, 20 WASH. U. J.L. & POL'Y 17, 25 (2006).

130. The New Deal reinforced an existing paradigm between the deserving and undeserving poor. *See* LINDA GORDON, PITIED BUT NOT ENTITLED: SINGLE MOTHERS AND THE HISTORY OF WELFARE 291 (1994). Social insurance programs designed for White working men, such as social security and UI, have generally carried no stigma, provided generous benefits pursuant to objective criteria, and been federally administered. *See id.* at 5–6, 145, 293–99. By contrast, cash assistance programs for single mothers, primarily Aid to Families with Dependent Children ("AFDC"), became stingy, stigmatized, state-administered, and discretionary. *Id.* at 293–94.

131. *See* MIMI ABRAMOVITZ, REGULATING THE LIVES OF WOMEN: SOCIAL WELFARE POLICY FROM COLONIAL TIMES TO THE PRESENT 323 (rev. ed. 1996); GUSTAFSON, *supra* note 12, at 21 ("The unstated but underlying goals of the rules were to police and punish the sexuality of single mothers, to close off the indirect access to government support of able-bodied men, to winnow the welfare rolls, and to reinforce the idea that families receiving aid were entitled to no more than near-desperate living standards.").

welfare rolls and push poor women, mostly of color, into the low-wage labor force."[132]

Welfare surveillance continues today in the Temporary Assistance to Needy Families ("TANF") program, in the form of drug tests, DNA tests, fingerprinting, extreme verification requirements, records matching, and various forms of highly personal questioning.[133] Khiara Bridges has written about the intrusive data gathering that poor, pregnant women face as a condition of receiving Medicaid; it involves detailed assessments regarding a woman's sexual history, prior substance use and abuse, past domestic violence, religious and cultural influences, emotional state, and strategies for preventing future pregnancies.[134] These interrogations "demonstrate that pathology is thought to attach to poor bodies in a way that it does not attach to wealthier bodies."[135] She concludes that "[t]o be poor is to be subject to invasions of privacy that we might understand as demonstrations of the danger of government power without limits."[136]

The specter of the welfare queen hovers over these surveillance practices and fuels the fear of fraud.[137] The welfare queen is a stereotype of a poor woman of color who cheats taxpayers while living an extravagant lifestyle at the taxpayer's expense and having too many children.[138] Attacks against welfare mothers reached a frenzy in the 1980s when President Reagan famously referred to welfare recipients as Cadillac driving "welfare queens."[139] Reagan repeatedly relayed the story of the "Chicago welfare queen" — a woman "who has eighty names, thirty addresses, twelve social security cards[,] and is collecting veterans' benefits on four non-existing deceased husbands . . . . Her tax-free cash income alone is over $150,000."[140] The woman on whom the story was apparently based, Linda Taylor, was indeed a con artist, and she was convicted in 1977 of welfare fraud for using two aliases to

---

132. *Supra* note 128, at 59.

133. *See* JOE SOSS, RICHARD C. FORDING & SANFORD F. SCHRAM, DISCIPLINING THE POOR: NEOLIBERAL PATERNALISM AND THE PERSISTENT POWER OF RACE 180 (2011) [hereinafter DISCIPLINING THE POOR].

134. BRIDGES, *supra* note 13, at 2–4, 7, 111. These questions are "neither immediately relevant to a doctor's ability to assess her health or relevant to her ability to successfully parent her child." *Id.* at 166. They are not posed to wealthier women. *Id.*

135. *Id.* at 113.

136. *Id.* at 5; *see also* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 2 (2021) ("[V]ulnerable groups are less able to absorb the social costs associated with privacy violations that may impact large swaths of people . . . .").

137. *See* BRIDGES, *supra* note 13, at 46.

138. *See* PREMILLA NADASEN, WELFARE WARRIORS: THE WELFARE RIGHTS MOVEMENT IN THE UNITED STATES 194–99, 239–40 (2005) (describing the roots of the stereotype); JOEL F. HANDLER & YEHESKEL HASENFELD, BLAME WELFARE, IGNORE POVERTY AND INEQUALITY 174–82 (2007).

139. LOU CANNON, PRESIDENT REAGAN: THE ROLE OF A LIFETIME 456–57 (2000); NADASEN, *supra* note 138, at 194–99, 239–40.

140. CANNON, *supra* note 139.

collect $8,000.[141] While there were some women who abused the welfare system — just as there are wealthy tax cheats[142] — these isolated instances came to exemplify the typical welfare recipient in the public mind.

Indeed, studies show that a majority of Americans oppose welfare spending because they believe that Black people receive the majority of welfare benefits — they hold stereotypes of Black people as lazy, and the media reinforces these racial attitudes.[143] Politicians from both parties have found the welfare queen to be a convenient punching bag, framing welfare as a symbol of dependency.[144] However, the welfare queen was and remains a myth. The majority of mothers receiving welfare are White; welfare-receiving families are smaller than the average American family; TANF recipients marry at the same rates as other women; most recipients stay on welfare for a short time period; and TANF benefits are far too meager to support a decent lifestyle, to say nothing of a luxurious lifestyle.[145]

Nevertheless, the welfare queen plays a featured role in judicial opinions. In the 1971 case of *Wyman v. James*,[146] the Supreme Court upheld the practice of government agents visiting and searching the homes of welfare applicants.[147] The Court rejected the argument that the visits searches conducted in violation of the Fourth Amendment,

---

141. Josh Levin, *The Welfare Queen*, SLATE (Dec. 19, 2013, at 12:41 ET), https://www.slate.com/articles/news_and_politics/history/2013/12/linda_taylor_welfare_queen_ronald_reagan_made_her_a_notorious_american_villain.html [https://perma.cc/JW4E-PYDX] ("The plural of anecdote is not data. The plural of the craziest anecdote you've ever heard is definitely not data. And yet, the story of the welfare queen instantly infected the policy debate over welfare reform.").

142. *See* Francine J. Lipman, *Tax Audits, Economics, and Racism*, OXFORD RSCH. ECON. & FIN. (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3956191 [https://perma.cc/Z9LX-7LF8].

143. MARTIN GILENS, WHY AMERICANS HATE WELFARE: RACE, MEDIA, AND THE POLITICS OF ANTIPOVERTY POLICY 3 (1999); *see also* Kirill Zhirkov, Kristin Lunz Trujillo & C. Daniel Myers, *Measuring Support for Welfare Policies: Implications for the Effects of Race and Deservingness Stereotypes*, 12 J. EXPERIMENTAL POL. SCI. 126, 127 (2025) (showing that stereotypes about race "significantly and consistently predict welfare opinions"); Jazmin L. Brown-Iannuzzi, Erin Cooley, Stephanie E. McKee & Charly Hyden, *Wealthy Whites and Poor Blacks: Implicit Associations between Racial Groups and Wealth Predict Explicit Opposition toward Helping the Poor*, 82 J. EXPERIMENTAL SOC. PSYCH. 26, 26–27 (2019) (arguing that automatic associations between race and social class predict policy attitudes toward wealth redistribution).

144. Michele Estrin Gilman, *The Return of the Welfare Queen*, 22 J. GENDER, SOC. POL'Y & L. 247, 249–52 (2014) (describing how during the 2012 Presidential campaign, candidates Mitt Romney (R) and Barack Obama (D) both sought to portray themselves as tough on welfare).

145. *See id.* at 262–66.

146. 400 U.S. 309 (1971).

147. *Id.* For an in-depth analysis of the privacy rights of welfare recipients, see generally Michele Estrin Gilman, *Welfare, Privacy, and Feminism*, 39 U. BALT. L.F. 1 (2009) and Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389 (2012).

reasoning that they were consensual,[148] which is doubtful given the pressure facing a poor mother needing food and a roof over her family's head.[149] Further, the Court held that even if the home visits were searches, they were reasonable given the state's need to protect the children of welfare mothers and its interest in deterring fraud.[150] The Court bolstered these unproven assumptions by attacking Ms. James, commenting on her "attitude," "evasiveness," and "belligerency" — all of which arose from her entirely reasonable belief that the state could verify her eligibility through personal interviews and documents in lieu of a home visit.[151] Ms. James asked to be treated the same as other beneficiaries of governmental largesse — none of whom had government agents at their door.[152] In dissent, Justice Douglas noted the double standard facing the poor: "If the welfare recipient was not Barbara James but a prominent, affluent cotton or wheat farmer receiving benefit payments for not growing crops, would not the approach be different? Welfare in aid of dependent children, like social security and unemployment benefits, has an aura of suspicion."[153]

Over fifty years after *Wyman*, this "aura of suspicion" still pervades public benefits programs and is used to justify a range of punitive surveillance technologies that criminalize poverty. For instance, the

148. *See Wyman*, 400 U.S. at 317–18.

149. *See* BRIDGES, *supra* note 13, at 10.

150. *Wyman*, 400 U.S. at 318–24. The Court was more skeptical of the alleged link between fraud and poverty a year later, in *U.S. Department of Agriculture v. Moreno*, 413 U.S. 528 (1973), when it struck down a rule denying food stamps to households containing unrelated individuals, holding the restriction did not bear a rational basis to Congress's purported justification of combatting fraud. However, this vigorous application of rational basis has not stood the test of time. *See, e.g.*, Lyng v. Castillo, 477 U.S. 635 (1986) (potential for fraud in the food stamp program supported legislative definition of "household" for eligibility purposes); Turner v. Glickman, 207 F.3d 419, 423 (7th Cir. 2000) (upholding statute permanently disqualifying people convicted of certain drug-related felonies from food stamps and welfare because requirement was rationally related to fighting fraud); Price v. Cohen, 715 F.2d 87 (3d Cir. 1983) (age restrictions for welfare eligibility upheld in part because state has legitimate interest in combatting fraud). *But see* CTIA — Wireless Ass'n. v. Echols, No. 13-CV-399, 2013 WL 663317 (N.D. Ga. 2013) (holding that need to combat fraud does not justify an increased rate regulation on telephone service for low-income people); Greenstein by Horowitz v. Bane, 833 F. Supp. 1054 (S.D.N.Y. 1993) (striking down a Medicaid policy argued to prevent fraud); Roberts v. Austin, 632 F.2d 1202 (5th Cir. Unit B 1980) (state agency cannot share food stamp claimants' data with state prosecutor seeking to review them to identify fraud without reasonable suspicion).

151. *Wyman*, 400 U.S. at 322 n.9.

152. *Id.* at 331–32 (Douglas, J., dissenting).

153. *Id.* at 332 (Douglas, J., dissenting). In 2007, the Ninth Circuit upheld the legality of welfare home visits in the context of TANF (the program that replaced AFDC, which was in effect during the *Wyman* case). Sanchez v. San Diego, 464 F.3d 916 (9th Cir. 2006), *reh'g en banc denied*, 483 F.3d 965 (9th Cir. 2007). The court expressly lumped welfare mothers with criminals on probation and concluded that neither group had a reasonable expectation of privacy. *Id.* at 926–27. In turn, this prompted a bitter dissent from a denial of a petition for rehearing en banc, in which seven Ninth Circuit judges called the case "nothing less than an attack on the poor," who are required "to sacrifice their dignity and their right to privacy." *Id.* at 969 (Pregerson, J., dissenting).

Medicaid program governing home-based health care tracks caregivers and service recipients through Electronic Visit Verification ("EVV") apps that must be installed on caregiver cell phones. Mandated by the federal government to prevent "fraud, waste, and abuse," EVV systems work by inspecting how workers spend their time in order to identify discrepancies.[154] Yet, as Alexandra Mateescu writes, this scrutiny shifts workers' focus from care to compliance.[155] Her study showed that "as workers struggled to make their work visible to digital systems; slight missteps in compliance often led to delayed or lost wages."[156] EVV systems put "a significant burden of proof on workers to show they are not engaging in 'time theft,'" yet location data has no correlation to quality of care.[157] For their part, service recipients report that EVV makes them feel as if they are under house arrest; they experience "pervasive fears that any deviations could invite scrutiny or, in the worst case, be used as grounds to cut hours or disqualify them from receiving services."[158] Automated systems such as EVV, which are built around fraud detection, harm people not only by generating false accusations, but also by instilling the *fear* of a false accusation, which in turn chills and shapes behavior in ways that undermine the very purpose of the social welfare program.

Public housing surveillance is yet another example of a mismatch between purported surveillance goals and outcomes. In public and subsidized housing, surveillance cameras and facial recognition technology monitor residents in the name of increasing safety.[159] The technologies are frequently used to nab residents for minor lease infractions, which in turn can lead to evictions.[160] One disabled tenant told the Washington Post that the housing authority threated her with eviction after a surveillance camera caught her sharing her key fob with an unauthorized guest; yet the guest was simply a friend bringing her groceries.[161] Clearly, surveillance cameras do not show the entire context of a situation, leading to the risk of misinterpretation.[162] Further, facial

154. Alexandra Mateescu, *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care*, DATA & SOC'Y, 16 (2021), https://datasociety.net/library/electronic-visit-verification-the-weight-of-surveillance-and-the-fracturing-of-care [https://perma.cc/B32L-8A7N].

155. *Id.* at 3.

156. *Id.* at 8.

157. *Id.* at 30.

158. *Id.* at 39.

159. *See* Michele Y. Ewert, *The Dangers of Facial Recognition Technology in Subsidized Housing*, 25 N.Y.U. J. LEGIS. & PUB. POL'Y 665, 673–77 (2023).

160. Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, WASH. POST (May 16, 2023, at 06:03 ET), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/ [https://perma.cc/8NKS-N4V7].

161. *Id.*

162. Lisa Lucile Owens, *Concentrated Surveillance Without Constitutional Privacy: Law, Inequality, and Public Housing*, 34 STAN. L. & POL'Y REV. 131, 137 (2023).

recognition technologies have lower rates of accuracy for people of color, especially women, who constitute the majority of residents in many urban housing projects.[163] Under the watchful eye of these technologies, residents are chilled in their ability to organize effectively for their rights as tenants.[164] In addition, public housing authorities share information gathered by these technologies with the police, which in turn multiplies police-resident interactions and expands the scope of carceral state.[165] Michelle Ewert describes this "'regulatory intersectionality,' in which subsidized housing providers, public benefits agencies, and other social welfare programs exchange information with law enforcement, destabiliz[ing] families through additional contact with the criminal law system."[166] Not surprisingly, many residents report the degrading feeling of living in a prison — and indeed, in some developments, the number of cameras outnumbers the ratio of those deployed in prisons.[167]

Fraud detection algorithms are less visible to claimants than smartphone apps and surveillance cameras, but share similar traits to these surveillance systems, particularly in criminalizing and stigmatizing poverty. These systems reveal that welfare is not about ensuring the well-being of vulnerable families. Rather, as Kaaryn Gustafson writes, "Policing the poor and protecting taxpayer dollars from fraud and abuse have taken priority over providing security to economically vulnerable parents and children."[168] This is a fraud-first, rather than a support-first, approach.

B. The Facts of Welfare Fraud

As *Wyman* reflects, fraud prevention has been a primary justification underlying welfare surveillance for decades. And the rhetoric is effective: In a 2021 public opinion poll, almost sixty percent of people stated that "it was very or somewhat common for people" to commit

163. Ewert, *supra* note 159, at 677; Owens, *supra* note 162, at 141 (noting that cameras are concentrated within neighborhoods whose residents are primarily of color).

164. Ewert, *supra* note 159, at 682–84.

165. Owens, *supra* note 162, at 140–43.

166. Ewert, *supra* note 159, at 683.

167. MacMillan, *supra* note 160. For yet another form of surveillance, see Dave Maass, *County Welfare Office Violated Accountability Rules While Surveilling Benefits Recipients*, ELEC. FRONTIER FOUND. (July 31, 2018), https://www.eff.org/deeplinks/2018/07/county-welfare-office-violated-accountability-rules-while-surveilling-benefits [https://perma.cc/V6PD-KD7H] (reporting on Sacramento County Department of Human Assistance employees who accessed data from automated license plate readers in tracking welfare recipients to search for fraud).

168. GUSTAFSON, *supra* note 12, at 1.

fraud to receive food stamps.[169] While protecting the public fisc is one of government's obligations, the government's core purpose is to serve the welfare of its citizens. Yet many surveillance practices assume criminality on the part of program participants, an assumption that is not empirically warranted or legally permitted. This Section reviews the empirical evidence about recipient fraud in three large safety net programs: Supplemental Nutrition Assistance Program ("SNAP"), Medicaid, and UI. It also reviews the significantly smaller, but politically potent TANF program.

Overall, while federal government agencies are statutorily required to track improper payments, they do not assess what proportion of those payments result from fraud.[170] The available evidence consistently shows that while overpayments and underpayments are endemic problems, recipients commit intentional fraud at very low rates. Overall, most overpayments result from mistakes by claimants and case workers in complying with inordinately complex program requirements.[171] This terrain has shifted since the pandemic, when criminal syndicates took advantage of weak data security to steal benefits — but it remains the case that needy Americans are not committing widespread fraud.

1. SNAP

SNAP, commonly known as food stamps, is the federal government's third largest public assistance program for low-income people. In 2023, 42.1 million people, or 12.6 percent of the population, received SNAP benefits per month,[172] and the federal government spent $112.8 billion on SNAP benefits.[173] This translates into an average monthly

169. Mark Robert Rank, Lawrence M. Eppard & Heather E. Bullock, *Welfare Fraud is Actually Rare, No Matter What the Myths and Stereotypes Say*, SALON (Apr. 4, 2021, at 06:30 EDT), https://www.salon.com/2021/04/04/welfare-fraud-is-actually-rare-no-matter-what-the-myths-and-stereotypes-say/ [https://perma.cc/AZT2-6UCE].

170. U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107487, MEDICARE AND MEDICAID: ADDITIONAL ACTIONS NEEDED TO ENHANCE PROGRAM INTEGRITY AND SAVE BILLIONS 8 (2024).

171. Fraud allegations are disproportionately high for people with limited English proficiency and people with disabilities. NEWSTROM & BLOCK, *supra* note 56, at 4 ("[C]ommunication barriers rooted in counties' failures to provide language and disability accommodations required by law are at the heart of many welfare fraud allegations.").

172. JORDAN W. JONES, U.S. DEPT. OF AGRIC. ECON. RSCH. SERV., SNAP SPENDING ROSE AND FELL WITH PANDEMIC-ERA CHANGES TO BENEFIT AMOUNTS (2024), https://www.ers.usda.gov/amber-waves/2024/june/snap-spending-rose-and-fell-with-pandemic-era-changes-to-benefit-amounts/ [https://perma.cc/3FEP-WKVL].

173. *Id.* The federal government pays the full cost of SNAP benefits and splits the cost of administering the program with the states, which operate it. *See* CTR. ON BUDGET & POL'Y PRIORITIES, POLICY BASICS: THE SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM (SNAP) (June 9, 2022), https://www.cbpp.org/research/policy-basics-the-supplemental-nutrition-assistance-program-snap [https://perma.cc/TD6L-T76P].

benefit amount of $188.45 per person and $350.89 per household,[174] which is delivered on electronic benefit transfer ("EBT") cards.[175] SNAP has strong anti-poverty effects: Prior to the pandemic it kept 6.6 million people, including three million children, above the poverty line.[176] To obtain SNAP, each applicant is interviewed by a state eligibility worker who then verifies the information provided, typically through automated data matching.[177] Recipients must reapply periodically, and they are required to report income changes impacting eligibility.[178] Under the SNAP quality control system, states must audit a representative sample of SNAP cases for accuracy, and federal officials then review a subset of those cases.[179]

The most frequently cited rate of SNAP fraud involves retailer trafficking in benefits, or the illegal sale of SNAP benefits for cash or other ineligible items, which is about 1.5 percent and disproportionately committed by small convenience stores.[180] By contrast, there are no reliable data on recipient trafficking.[181] In 2019, the SNAP overpayment rate, or benefit dollars issued to ineligible households or to eligible households above permitted amounts, was 6.18 percent, while the underpayment rate, or benefits amounts lower than permitted amounts, was 1.18 percent.[182] However, the United States Department of Agriculture,

---

174. *See* Drew Desilver, *What the Data Says About Food Stamps in the U.S.*, PEW RSCH. CTR. (July 19, 2023), https://www.pewresearch.org/short-reads/2023/07/19/what-the-data-says-about-food-stamps-in-the-u-s/ [https://perma.cc/4XA7-UAGY].

175. Rosalie A. Peng, *A Snapshot of the Pandemic-Era SNAP Program and the Upcoming 2023 Farm Bill*, GEO. J. ON POVERTY L. & POL'Y (2023), https://www.law.georgetown.edu/poverty-journal/blog/a-snapshot-of-the-pandemic-era-snap-program-and-the-upcoming-2023-farm-bill/ [https://perma.cc/V8NB-PBQK].

176. CTR. ON BUDGET & POL'Y PRIORITIES, *supra* note 173.

177. U.S. DEPT. OF AGRIC., ASSESSMENT OF STATES' USE OF COMPUTER MATCHING PROTOCOLS IN THE SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM (2020), https://fns-prod.azureedge.us/sites/default/files/resource-files/SNAPComputerMatching-Summary.pdf [https://perma.cc/XU92-ABM6].

178. CTR. ON BUDGET & POL'Y PRIORITIES, *supra* note 173.

179. *Id.*

180. Press Release, U.S. Dept. of Agric., USDA Announces New Report on Trafficking and Announces Additional Measures to Improve Integrity in the Supplemental Nutrition Assistance Program (Aug. 15, 2013), https://www.fns.usda.gov/pressrelease/2013/fns-001213 [https://perma.cc/TTT5-4USL]; RANDY ALISON AUSSENBERG, CONG. RESCH. SERV., ERRORS AND FRAUD IN THE SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM 2, 6 (2018). These stores struggle with compliance, and their disqualification from the program can adversely impact food access in low-income neighborhoods. H. Claire Brown, *How an Algorithm Kicks Small Businesses Out of the Food Stamps Program on Dubious Fraud Charges*, COUNTER (Oct. 8, 2018, at 09:00 ET), https://thecounter.org/usda-algorithm-food-stamp-snap-fraud-small-businesses/ [https://perma.cc/5EUD-EXJ9].

181. AUSSENBERG, *supra* note 180, at 10–11 (explaining states lack a standardized manner of tracking and reporting fraud).

182. Dottie Rosenbaum & Katie Bergh, *SNAP Includes Extensive Payment Accuracy System*, CTR. ON BUDGET AND POL'Y PRIORITIES, at 2 (June 21, 2024), https://www.cbpp.org/research/food-assistance/snap-includes-an-extensive-payment-accuracy-system [https://perma.cc/BAB6-V6MY]. The underpayment rate is underestimated, and states are not penalized for underpayments as they are for overpayments. *Id.*

which oversees the SNAP program, consistently cautions that overpayments are not synonymous with fraud,[183] and indeed, the majority of SNAP overpayments result when recipients, state workers or computer programmers make mistakes as they navigate complex regulatory requirements.[184] Recipients who receive an overpayment are required to repay the sum regardless of the cause, although there are available waivers in cases of financial hardship.[185]

During the pandemic, Congress suspended quality control reviews and gave states greater program flexibility to meet surging need, which in turn appears to have led to more payment errors.[186] For fiscal year 2022, states had an overpayment rate of 9.84 percent and an underpayment rate of 1.7 percent,[187] spurring the congressional leaders of the House and Senate Agriculture Committees to denounce the error rate as "unacceptable" and to call on governors and administrators "to improve their program operations, remain accountable to the taxpayer, and most importantly, ensure that benefits are targeted to the people who are the most in need."[188] Interestingly, public support for SNAP increased during the pandemic as recently unemployed people poured into the SNAP program.[189] Media narratives also pivoted radically. Before the pandemic, media reporting about SNAP focused on stories about fraud and abuse, "along with the occasional mugshot of people accused of fraud."[190] This abruptly stopped during the pandemic; when

183. U.S. DEPT. OF AGRIC., ENSURING ELIGIBLE SNAP HOUSEHOLDS GET THE RIGHT BENEFITS (2024), https://www.fns.usda.gov/snap/quality-control [https://perma.cc/2DB9-SZ65]; AUSSENBERG, *supra* note 180, at 2 ("Errors are not the same as fraud. Fraud is intentional activity that breaks federal and/or state laws, while errors can be the result of unintentional mistakes. Certain acts, such as trafficking SNAP benefits, are always considered fraud; other acts, such as duplicate enrollment, may be the result of either error or fraud depending on the circumstances of the case.").

184. *Supra* note 182, at 5; AUSSENBERG, *supra* note 180, at 10 ("There is currently no single standard measurement that individually quantifies the extent of recipient errors, recipient fraud, or agency errors."); Stacy Dean, Testimony Before the Subcomms. on Intergovernmental Affairs & Health Care, House Comm. on Oversight & Gov't Reform (May 9, 2018), https://www.cbpp.org/program-integrity-for-the-supplemental-nutrition-assistance-program [https://perma.cc/BG6A-FJZJ] ("In addition, states have reported that almost 60 percent of the dollar value of overpayments and almost 90 percent of the dollar value of underpayments were their fault, rather than recipients'. Much of the rest of overpayments resulted from innocent errors by households facing a program with complex rules.").

185. AUSSENBERG, *supra* note 180, at 21.

186. *Supra* note 182.

187. *Id.*

188. Press Release, Britton T. Burdick, House Agriculture Committee Democrats, Joint Statement on SNAP Payment Error Rate (June 30, 2023), https://democrats-agriculture.house.gov/news/documentsingle.aspx?DocumentID=2810 [https://perma.cc/ENQ4-JSN5].

189. Saul Elbein, *Majority of Voters Want SNAP Increased, Not Cut: Poll*, HILL (July 17, 2023, at 14:47 ET), https://thehill.com/homenews/senate/4101853-majority-of-voters-want-snap-increased-not-cut-poll/ [https://perma.cc/ZQ5A-A822].

190. Pamela Mejia, Hina Mahmood, Sarah B. Perez-Sanz, Kim Garcia & Lori Dorfman, *"People Like Us": News Coverage of Food Assistance During the COVID-19 Pandemic*, 6 HEALTH EQUITY 367, 372 (2022).

the media reported on families receiving SNAP they used "language that evoked empathy for recipients, framing them as 'people like us.'"[191] Notions of deservingness profoundly shape narratives about welfare fraud.

Under the second Trump Administration, the U.S. Department of Agriculture ("USDA") demanded that states and third-party vendors turn over SNAP recipients' personal data, including social security numbers and addresses, in order to carry out President Trump's Executive Order on "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos."[192] States were threatened with a loss of funds for noncompliance. A coalition of privacy and hunger groups sued to block the effort, alleging it violated federal privacy and other laws.[193] In May 2025, USDA told the court it was temporarily halting the effort until it addressed legal safeguards for data privacy.[194]

2. Medicaid

With regard to Medicaid, which provides health insurance for low-income and disabled people, research has shown that the bulk of fraudulent activity is committed by health care providers[195] — not by the approximately ninety million needy people (or one in five Americans) that use the program.[196] The program is jointly funded by the federal

---

191. *Id.*; *see also* PETER H. SCHUCK & RICHARD J. ZECKHAUSER, TARGETING IN SOCIAL PROGRAMS: AVOIDING BAD BETS, REMOVING BAD APPLES 34–36 (2010) (describing that the adoption of welfare reform legislation in 1996, which contained stringent work requirements, was associated with fewer negative stories in the media about welfare recipients).

192. Exec. Order No. 14243, 90 Fed. Reg. 13, 681 (Mar. 20, 2025).

193. Complaint, Namod Pallek et al. v. Brooke Rollins et al., Civ. No. 1:25-cv-01650 (D.D.C. May 22, 2025), https://protectdemocracy.org/wp-content/uploads/2025/05/USDA_SNAP_Complaint.pdf [https://perma.cc/CP92-LGEL].

194. *See* Aliss Higham, *Trump Administration Backs off Demand for SNAP Recipient Data*, NEWSWEEK (June 4, 2025, at 09:01 ET), https://www.newsweek.com/trump-administration-backs-off-demand-snap-recipients-data-2080714 [https://perma.cc/R43L-C3Z3].

195. Andy Schneider, *The Truth About Fraud Against Medicaid*, GEO. U. MCCOURT SCH. OF PUB. POL'Y: BLOG (Jan. 10, 2025), https://ccf.georgetown.edu/2025/01/10/the-truth-about-fraud-against-medicaid/ [https://perma.cc/MQ9Z-FUUE]; *see also* Elizabeth Hinton, Jessica Mathers & Robin Rudowitz, *5 Key Facts About Medicaid Program Integrity – Fraud, Waste, Abuse and Improper Payments*, KAISER FAM. FOUND. (Mar. 18, 2025) https://www.kff.org/medicaid/5-key-facts-about-medicaid-program-integrity-fraud-waste-abuse-and-improper-payments/ [https://perma.cc/SSJ9-H32J] ("What is known about fraud in Medicaid is that it's not unique to Medicaid (fraud also occurs in Medicare and private health insurance) and is mostly committed by providers.").

196. Robin Rudowitz, Alice Burns, Elizabeth Hinton & Maiss Mohamed, *10 Things to Know About Medicaid*, KAISER FAM. FOUND. (Feb. 18, 2025), https://www.kff.org/medicaid/issue-brief/10-things-to-know-about-medicaid/ [https://perma.cc/7ARC-TDFX]. The Medicare program also faces high rates of fraud committed by medical providers, but its care workers are not surveilled like those in the Medicaid program, likely reflecting that the latter program serves the poor. *See* Mateescu, *supra* note 154.

government and the states and administered by the states pursuant to federal guidelines.[197] Medicaid in 2024 was a $919 billion program,[198] and estimates are that improper payments cost about $31 billion a year, or 5.1 percent of overall spending.[199] Almost 80 percent of improper payments result from insufficient documentation, "and do not necessarily indicate fraud or abuse."[200] Intentionally fraudulent schemes involve identity theft or fabricated data, "used to create false victims of disease or addiction."[201] Indeed, "the biggest problem in health care fraud is not pseudopatients, but rather the doctors who enable, enlist, or fabricate them."[202] Such fraud is "not only lucrative and complex, but also long-term."[203]

In sum, "the people most likely to bilk the system are doctors and medical providers — and not so-called 'welfare queens.'"[204] Indeed, under Medicaid, monetary benefits flow directly to providers, and beneficiaries never touch funds directly. Perhaps as a result, the welfare queen myth does not permeate Medicaid as much as other support programs. Over seventy percent of Americans held favorable opinions of Medicaid.[205] Nevertheless, in 2025, Congress passed and President Trump signed a bill cutting Medicaid spending and including unnecessary work requirements and onerous paperwork requirements for Medicaid recipients using the specter of "fraud" to justify the legislation. The legislation is predicted to result in the loss of coverage for millions of needy Americans and the closure of rural hospitals.[206]

---

197. Rudowitz et al., *supra* note 196.

198. Elizabeth Williams, Alice Burns, Anna Mudumala & Robin Rudowitz, *Medicaid Financing: The Basics*, KAISER FAM. FOUND. (Mar. 4, 2026) https://www.kff.org/medicaid/medicaid-financing-the-basics/#870ed126-45c3-4465-8b9a-ae0eea487dcf [https://perma.cc/K8PX-4HKT].

199. Hinton et al., *supra* note 195.

200. Hinton et al., *supra* note 195; *Fiscal Year 2024 Improper Payments Fact Sheet*, CMS NEWSROOM (Nov. 15, 2024), https://www.cms.gov/newsroom/fact-sheets/fiscal-year-2024-improper-payments-fact-sheet [https://perma.cc/7DWP-BUCT].

201. John O. Savino & Brent E. Turvey, *Medicaid/Medicare Fraud*, *in* FALSE ALLEGATIONS: INVESTIGATIVE AND FORENSIC ISSUES IN FRAUDULENT REPORTS 95 (Brent E. Turvey, John O. Savino & Aurelio Coronado Mares eds. 2018).

202. *Id.* at 95; *see also* Schneider, *supra* note 195 (noting that the federal government reported convictions against "ambulance service providers, durable medical equipment suppliers, diagnostic labs, nursing homes, pain clinics, pharmacies, physical therapists, physicians, and substance use treatment providers" — but not a single beneficiary).

203. SAVINO, *supra* note 201, at 107.

204. *Id.* at 96.

205. Rudowitz et al., *supra* note 196.

206. *See* Alicia Parlapiano & Margot Sanger-Katz, *9 Questions About the Republican Megabill, Answered*, N.Y. TIMES (July 3, 2025), https://www.nytimes.com/2025/07/03/upshot/republican-bill-faq.html [https://perma.cc/H5NK-9DSV]; Linda Qiu, *Trump and Allies Sell Domestic Policy Bill With Falsehoods*, N.Y. TIMES (June 2, 2025), https://www.nytimes.com/2025/06/02/us/politics/trump-big-beautiful-bill-facts.html [https://perma.cc/KN8B-GVW2]; David Wright & Eva McKend, *Rural Health Clinics are*

3. Unemployment Insurance

Unemployment insurance is designed to support people who are laid off from their jobs while they seek new employment and to stabilize the economy in times of recession or crisis.[207] States administer and largely fund UI with oversight from the federal Department of Labor.[208] UI generally provides twenty-six weeks of benefits to unemployment workers in an amount of about half their wages, up to a maximum level.[209] During the pandemic, UI demand soared as millions of workers lost their jobs.[210] Congress expanded the program in several ways: it funded a supplemental benefits amount, extended the time period for receipt of benefits, and granted benefits to self-employed workers for the first time.[211] These expansions have since ended.[212]

As of 2026, the improper payment rate exceeded ten percent for seventeen of the prior twenty years, yet — as with other governmental assistance programs — intentional fraud estimates are much lower.[213] The "improper payment" rate for 2019, before the pandemic, was 10.6 percent.[214] In 2021, the improper payment rate soared to 17.9 percent, for a total of $73.8 billion in improper payments across the various existing and new UI programs.[215]

For "regular" UI, fraud is defined at the state level;[216] however, during the pandemic, several of the emergency federal laws related to

---

Closing After Trump's "One Big Beautiful Bill," Raising the Legislation's Political Risks, CNN (Sep. 22, 2025), https://www.cnn.com/2025/09/22/politics/rural-healthcare-one-big-beautiful-bill [https://perma.cc/AW7F-6G8D].

207. CONG. RSCH. SERV., THE FUNDAMENTALS OF UNEMPLOYMENT COMPENSATION (2026), https://crsreports.congress.gov/product/pdf/IF/IF10336 [https://perma.cc/MF5R-7HYL].

208. CONG. RSCH. SERV., UNEMPLOYMENT INSURANCE: PROGRAM INTEGRITY AND FRAUD CONCERNS RELATED TO THE COVID-19 PANDEMIC RESPONSE 1 (2022), https://crsreports.congress.gov/product/pdf/R/R47079 [https://perma.cc/WQ8F-6793] (noting that the program is funded primarily with state unemployment taxes).

209. CONG. RSCH. SERV., FUNDAMENTALS, *supra* note 207.

210. CONG. RSCH. SERV., INTEGRITY AND FRAUD, *supra* note 208, at 4.

211. CONG. RSCH. SERV., FUNDAMENTALS, *supra* note 207.

212. *Id.*

213. *Id.*; U.S. DEP'T. OF LABOR, OFF. OF INSPECTOR GEN., OIG OVERSIGHT OF THE UNEMPLOYMENT INSURANCE PROGRAM n.16 (2025), https://oig.dol.gov/doloiguioversightwork.htm [https://perma.cc/YT68-A6GF] (noting that intentional fraud is one of four causes of overpayments, and before the pandemic, amounted to about one-quarter of overpayments).

214. U.S. GOV'T ACCOUNTABILITY OFF., TESTIMONY BEFORE THE COMM. ON WAYS AND MEANS, HOUSE OF REP., STATEMENT OF GENE L. DODARO 19 (2023), https://www.gao.gov/assets/gao-23-106586.pdf [https://perma.cc/6GHG-6KC2].

215. CONG. RSCH. SERV., UNEMPLOYMENT INSURANCE PROGRAM INTEGRITY: RECENT DEVELOPMENTS (2022), https://crsreports.congress.gov/product/pdf/IF/IF12243 [https://perma.cc/Q7A7-NGG2].

216. CONG. RSCH. SERV., INTEGRITY AND FRAUD, *supra* note 208, at 6 ("States vary on the level of evidence required to demonstrate a knowing and willful act or the concealment of facts. An overpayment classified as a fraud overpayment in one state might be determined to be a nonfraud overpayment in another state.").

UI provided statutory definitions of fraud for the first time.[217] In general, fraud requires a "knowing and willful act or concealment of material facts to obtain or increase benefits."[218] States can recover overpayments by offsetting future UI benefits and through seizing federal and state tax refunds, and in cases of fraud, they may also impose fines and penalties.[219] However, states have the authority to waive non-fraud overpayments, particularly in cases of financial hardship.[220]

While the full extent of UI pandemic fraud is still being uncovered, the General Accountability Office estimates it as between $100 billion and $135 billion, or eleven to fifteen percent of the total UI benefits paid during the pandemic.[221] The pandemic increased UI fraud for several reasons. State agencies had reduced staff in the years prior to the pandemic, and federal funding for administration stagnated.[222] At the same time, IT systems were not adaptable to the expanded and new UI programs,[223] and even modernized systems struggled due to the scale of the crisis and the complexity of UI policies.[224] Demand from the public surged[225] as twenty-two million people found themselves out of work in the first two months of the shutdown.[226] Forced to pivot to a purely online application system, states were unable to establish effective and accurate digital identity verification systems.[227]

Criminal syndicates swooped in to take advantage of the chaos, armed with hacked and stolen personal data.[228] Meanwhile, these same

---

217. CONG. RSCH. SERV., RECENT DEVELOPMENTS, *supra* note 215.

218. *Id.*

219. CONG. RSCH. SERV., INTEGRITY AND FRAUD, *supra* note 208, at 8.

220. *Id.*

221. U.S. GOV'T ACCOUNTABILITY OFF., UNEMPLOYMENT INSURANCE: ESTIMATED AMOUNT OF FRAUD DURING PANDEMIC LIKELY BETWEEN $100 BILLION AND $135 BILLION (2023), https://www.gao.gov/products/gao-23-106696 [https://perma.cc/R42M-4C43]; *see also* CONG. RSCH. SERV., INTEGRITY AND FRAUD, *supra* note 208, at 8–11 (reporting on various fraud estimates).

222. CONG. RSCH. SERV., INTEGRITY AND FRAUD, *supra* note 208, at 12.

223. CONG. RSCH. SERV., RECENT DEVELOPMENTS, *supra* note 215.

224. JENNIFER PAHLKA, RECODING AMERICA: WHY GOVERNMENT IS FAILING IN THE DIGITAL AGE AND HOW WE CAN DO BETTER 52–54 (2023).

225. CONG. RSCH. SERV., INTEGRITY AND FRAUD, *supra* note 208, at 14 (quoting testimony of the DOL Inspector General to Congress stating that within two to three weeks of the COVID shutdown in March 2020, "initial claims rose to 10 times pre-pandemic levels, far higher than state systems were designed to handle. Within 5 months, through August 15, 2020, the Department reported 57.4 million initial claims, the largest increase since the Department began tracking UI data in 1967.").

226. Nicole Bateman & Martha Ross, *The Pandemic Hurt Low-Wage Workers the Most — and So Far, the Recovery Has Helped Them the Least*, BROOKINGS (July 28, 2021), https://www.brookings.edu/articles/the-pandemic-hurt-low-wage-workers-the-most-and-so-far-the-recovery-has-helped-them-the-least/ [https://perma.cc/7WCF-MKJP].

227. Gilman, *supra* note 15, at 310–11.

228. CONG. RSCH. SERV., INTEGRITY AND FRAUD, *supra* note 208, at 19 ("Since the onset of the Coronavirus Disease 2019 (COVID-19) pandemic, the UI program has been an attractive target for international and domestic criminal organizations perpetrating identity fraud.");

dynamics made it difficult for eligible claimants to access benefits. The media was flush with stories of recently unemployed people grappling with UI websites that froze, crashed, flashed error messages, and went offline at random hours.[229] In the face of collapsing systems, claimants were unable to get their calls to their state labor agencies answered by human beings.[230] Fraud skyrocketed, but it was not due to laid off workers.[231] It was mostly committed by domestic and foreign criminal syndicates taking advantage of the chaos.[232]

4. TANF

Estimating rates of TANF fraud raises a more complicated analysis. When people think of "welfare," they are likely referring to TANF.[233] It is the primary program providing cash assistance to very low-income families, but its political salience far outstrips its numbers.[234] TANF is a tiny program in comparison to those noted above; cash assistance benefits served just 2.8 million people nationwide in 2023, of which 1.9 million were children.[235] It is funded jointly by the federal and state governments, which spent $31.3 billion in fiscal year 2022. However, of that sum, only twenty-three percent was spent on cash assistance; the bulk of the funds are spent on a variety of welfare-to-work services and activities such as Head Start and employment services. The maximum amount of benefits varies by state; the average is $517 per month.[236] Low benefit levels are tied to welfare's racist

---

PAHLKA, *supra* note 224, at 71 ("[C]laims filed in bulk by organized crime, with their perfectly matched data, were sailing through the system."); NAT'L ACAD. OF SOC. INS., UNEMPLOYMENT INSURANCE TASK FORCE: FINAL REPORT 15 (2024), https://www.nasi.org/wp-content/uploads/2024/07/Unemployment-Insurance-Task-Force-Final-Report.pdf [https://perma.cc/Y4A7-V5LP].

229. Gilman, *supra* note 15, at 311.

230. *Id.*

231. An audit in California during this timeframe found that only "0.2 percent of applicants who were flagged for identity verification turned out to be committing fraud." PAHLKA, *supra* note 215, at 70–71.

232. Gilman, *supra* note 15, at 311.

233. *See* GUSTAFSON, *supra* note 9, at 44.

234. Diana Azevedo-McCaffrey & Tonanziht Aguas, *Continued Increases in TANF Benefit Levels Are Critical to Helping Families Meet Their Needs and Thrive*, CTR. ON BUDGET & POL'Y PRIORITIES (May 29, 2024), https://www.cbpp.org/research/income-security/continued-increases-in-tanf-benefit-levels-are-critical-to-helping [https://perma.cc/ZR3A-W7NR].

235. CONG. RSCH. SERV., THE TEMPORARY ASSISTANCE FOR NEEDY FAMILIES (TANF) BLOCK GRANT: RESPONSES TO FREQUENTLY ASKED QUESTIONS 4–5 (2024), https://sgp.fas.org/crs/misc/RL32760.pdf [https://perma.cc/ZDU8-HZRX] ("During 2020, a year when the economy was affected by the COVID-19 pandemic, there was a brief uptick in the number of families receiving assistance. That response to the pandemic was short-lived.").

236. OFF. OF FAM. ASSISTANCE, OFA RELEASES FY 2021 CHARACTERISTICS AND FINANCIAL CIRCUMSTANCES OF TANF RECIPIENTS DATA (2023), https://acf.gov/ofa/news/ofa-releases-fy-2021-characteristics-and-financial-circumstances-

history,[237] with lower benefit amounts in states with larger Black population shares.[238]

Recipients cannot receive TANF for more than five years in their lifetime, and many states impose shorter time limits. Further, states must have fifty percent of the caseload engaged in work or work activities.[239] The work requirements were imposed in 1996, when TANF replaced the pre-existing program called AFDC, which was perceived as creating dependency among recipients. In addition to the work requirements, TANF also permits states to impose various behavioral requirements such as family caps (denying benefits to children born after TANF eligibility is established); drug testing; learnfare (tying benefits to school attendance); and a ban on receipt of benefits by people convicted of a felony.[240] These options are all founded on a belief that "parents seeking assistance are irresponsible, criminal, or undeserving of support."[241]

Despite the welfare queen narrative, the federal government does not require states to gather data on TANF overpayments.[242] Thus, we must turn to other sources for estimates of TANF fraud. Kaaryn Gustafson conducted an in-depth analysis of TANF fraud, using an ethnographic approach.[243] She found that some applicants do not report all their sources of income to the state.[244] Because it is impossible to survive on welfare benefits, which remain well below the poverty line, some welfare applicants accept unreported support from family members or earn additional income from jobs such as babysitting or cutting hair.[245] Welfare mothers are in a bind — they must earn unreported income to provide for their children, but this conduct is considered

---

tanf-recipients-data [https://perma.cc/X5QE-HPKH]; CONG. RSCH. SERV., FAQS*, supra* note 235, at 6 ("In July 2022, the maximum monthly benefit for a family of two (single parent and one child) ranged from $915 in New Hampshire to $162 in Arkansas.").

237. Azevedo-McCaffrey & Aguas, *supra* note 234.

238. *Id.*

239. CONG. RSCH. SERV., FAQS, *supra* note 235, at 7.

240. Laura Meyer, Ife Floy & Ladonna Pavetti, *Ending Behavioral Requirements and Reproductive Control Measures Would Move TANF in an Antiracist Direction*, CTR. ON BUDGET & POL'Y PRIORITIES (Feb. 23, 2022), https://www.cbpp.org/research/income-security/ending-behavioral-requirements-and-reproductive-control-measures-would [https://perma.cc/J78W-XJWF].

241. *Id.*

242. U.S. Gov't ACCOUNTABILITY OFF., COVID-19: CURRENT AND FUTURE FEDERAL PREPAREDNESS REQUIRES FIXES TO IMPROVE HEALTH DATA AND ADDRESS IMPROPER PAYMENTS (Apr. 27, 2022), https://www.gao.gov/products/gao-22-105397 [https://perma.cc/J9AQ-TN6Z]. A bill has been proposed to change this. *See* Press Release, House Budget Committee, Chairman Arrington Introduces Legislation to Eliminate Fraud and Improper Payments in TANF (Feb. 28, 2024), https://budget.house.gov/press-release/chairman-arrington-introduces-legislation-to-eliminate-fraud-and-improper-payments-in-temporary-assistance-for-needy-families-tanf [https://perma.cc/TAS5-BFLJ].

243. *See* GUSTAFSON, *supra* note 9, at 2.

244. *Id.* at 3, 117.

245. *Id.* at 101–02.

"fraud."[246] Thus, the state's low welfare stipends and rigid earning limits can create the very fraud that the state seeks to eliminate.[247]

Further, some women convicted of welfare fraud fail to report income for circumstances out of their control, such as when their partners hide their income or force them to keep it secret.[248] And, as with other benefits programs, the bulk of so-called fraud cases are unintentional and occur when welfare applicants either do not understand the complex income and resource reporting rules of TANF, or are misinformed by their caseworkers. Notably, the jobs obtained by welfare mothers tend to be unstable with fluctuating schedules and incomes, which can also lead to reporting problems when anticipated and actual income differ. "In short, the U.S. system both produces and punishes lawbreakers."[249] Algorithms will not solve poverty or fill the gap between people's needs and the stingy level of benefits. They will only expose the gap in the name of fraud.

Notably, various surveillance tactics designed to expose welfare fraud have come up short. For instance, New York City began fingerprinting welfare applicants in 1995 in an effort to root out imagined fraud. However, the city found only forty-three cases of double dipping out of 148,000 recipients.[250] In Los Angeles County, a $9.6 million fingerprinting requirement for welfare applicants found only two cases of intentional fraud during its first four months of operation.[251]

Some states drug test welfare applicants, reflecting yet another form of surveillance based on the presumed criminality of recipients.[252] In thirteen states conducting welfare drug testing in 2019, 260,000

246. *Cf.* Stephen D'Arcy, *Is There Ever an Obligation to Commit Welfare Fraud?*, 42 J. VALUE INQUIRY 377, 387 (2008) (arguing that in some situations parents have a moral obligation to provide for their children even if it involves committing welfare fraud).

247. A California study found most fraud convictions were for unreported amounts of approximately $164 per month per household member, "suggesting that parents made repeated attempts to plug gaps in inadequate subsistence budgets." Richelle S. Swan, Linda L. Shaw, Sharon Cullity, Joni Halpern & Juliana Humphrey, *The Untold Story of Welfare Fraud*, 35 J. SOCIO. & SOC. WELFARE 133, 141–42 (2008).

248. NEWSTROM & BLOCK, *supra* note 56, at 5 (explaining that abusers often provide the state with false "tips" of welfare fraud to exert control over the victim or to gain an advantage); *see also* Swan et al., *supra* note 247, at 140.

249. Swan et al., *supra* note 247, at 140.

250. Kimberly J. McLarin, *Welfare Fingerprinting Finds Most People are Telling Truth*, N.Y. TIMES (Sep. 29, 1995), https://www.nytimes.com/1995/09/29/nyregion/welfare-fingerprinting-finds-most-people-are-telling-truth.html [https://perma.cc/69H9-FDK7].

251. *See* Hugo Martin, *County Welfare Recipients Fingerprinted: Social Services: Computer Finds Only Two Cases of Fraud but 700 People Have Refused to Participate in Controversial Program*, L.A. TIMES (Oct. 12, 1991), https://www.latimes.com/archives/la-xpm-1991-10-12-me-106-story.html [https://perma.cc/FW2L-ZBY9].

252. MAGGIE MCCARTY, GENE FALK, RANDY A. AUSSENBERG & DAVID H. CARPENTER, CONG. RSCH. SERV., DRUG TESTING AND CRIME-RELATED RESTRICTIONS IN TANF, SNAP, AND HOUSING ASSISTANCE 8 (2016), https://sgp.fas.org/crs/misc/R42394.pdf [https://perma.cc/48H2-Y9JT] ("A positive drug test generally makes that individual ineligible for TANF assistance. However, some states allow recipients to either retain eligibility or regain eligibility by participating in, or completing, a substance abuse treatment program.").

people were tested at a cost of $200,000, and only 338 people tested positive.[253] "In some states, not one person tested positive."[254] These programs are expensive, as is the welfare fraud investigative apparatus, and yet government does not measure these costs or assess whether they are justified by the outcomes. Gustafson found that in just one year, California spent $34 million to investigate TANF fraud yet identified only $19.6 million in overpayments.[255] Prosecution of welfare fraud generates additional costs for the criminal justice system, as incarcerating a mother for one-year costs well more than providing for her family. Moreover, when a mother is removed from her home, her children are likely to go into the foster care system, which also costs more than providing the family with cash assistance in the first instance and devastates families.[256] In short, state resources are going to welfare fraud prosecution rather than poverty alleviation.[257]

C. The Fraud Double Standard

The relentless focus on the "welfare queen" glosses over the valuable government assistance that flows to wealthier people and corporations, which receives far less scrutiny or public approbation. The top twenty percent of the population receives sixty-six percent of tax benefits, which include deductions, credits, and other federal tax write-offs.[258] The middle-class receive their proportionate share of government entitlements too, such as tax deductions for mortgages and retirement plans, and childcare tax credits — none of which are stigmatized like welfare.[259]

---

253. Amanda Michelle Gomez & Josh Israel, *What 13 States Discovered After Spending Hundreds of Thousands Drug Testing the Poor*, THINK PROGRESS (Apr. 26, 2019, at 11:59 ET), https://archive.thinkprogress.org/states-cost-drug-screening-testing-tanf-applicants-welfare-2018-results-data-0fe9649fa0f8/ [https://perma.cc/9JLP-XR5T].

254. *Id.*

255. GUSTAFSON, *supra* note 12, at 184.

256. *Id.* at 185. On the emotional and psychological harms suffered by children who are removed from their homes, see Shanta Trivedi, *The Harm of Child Removal*, 43 N.Y.U. REV. L. & SOC. CHANGE 523 (2019).

257. GUSTAFSON, *supra* note 12, at 185.

258. *See, e.g.*, *Distributional Effects of the Tax Provisions in the 2025 Budget Reconciliation Act*, TAX POL'Y CTR. (July 3, 2025), https://taxpolicycenter.org/tax-model-analysis/distributional-effects-tax-provisions-2025-budget-reconciliation-act [https://perma.cc/87WU-4JB8] (explaining that under the One Big Beautiful Bill Act enacted in 2025, nearly sixty percent of the law's tax benefits go the top twenty percent of earners (households with incomes over $217,000)); *see also* Dylan J.F. Bellisle, Gabrielle Pepin & Bethan L. Letiecq, *The Role of Taxation in Family Inequality: Possibilities for Reform*, NAT'L COUNCIL ON FAM. RELS. (Dec. 20, 2024), https://www.ncfr.org/policy/research-and-policy-briefs/role-of-taxation-family-inequality-possibilities-for-reform [https://perma.cc/BBP9-FYUE] ("Over the past 40 years, U.S. federal tax policy has shifted the tax burden away from wealthy families without providing comparable investments in the financial well-being of low- and moderate income families and their children through tax credits and deductions.").

259. Wendy A. Bach, *Poor Support/Rich Support: (Re)Viewing the American Social Welfare State*, 20 FLA. TAX REV. 495 (2017).

American businesses receive about 100 billion dollars a year in subsidies, and the government bailouts of the auto industry and Wall Street banks following the mid-aughts recession added hundreds of billions more to the taxpayers' tab when those entities failed.[260] Companies like Walmart and Amazon may be the true welfare queens, as state and local subsidies put billions of taxpayer dollars into their coffers every year.[261] At the same time, Walmart and fast-food giants like McDonalds pay poverty-level wages to their employees, thereby shifting the costs of those employees' food stamps and health care costs on taxpayers.[262]

Even when wealthy people and companies cheat the government, there are few public or political calls for retribution.[263] The federal income tax gap — generated from underreporting, underpayment, and non-filers — is estimated at $600 billion to $1 trillion annually, and "highest income taxpayers and largest corporations . . . are responsible for more than seventy percent of the tax gap."[264] The sum of the tax gap is larger than the costs of the social safety net.[265] Yet Congress has repeatedly defunded the IRS, particularly its enforcement arm.[266]

The odds of being prosecuted for welfare fraud are higher than for tax fraud: "[T]he average U.S. taxpayer's odds of being punished for fraud are roughly 1 in 443,000, while a California public benefits recipients' odds of being punished for alleged fraud are 1 in 117."[267] Similarly, a 2023 study of corporate fraud found that only one-third of corporate fraud is detected. Each year, on average, forty-one percent of large publicly traded firms commit accounting violations and ten

260. *See* Ilya Shapiro & Carl G. DeNigris, *Occupy Pennsylvania Avenue: How the Government's Unconstitutional Actions Hurt the 99 percent*, 60 DRAKE L. REV. 1085, 1103–04 (2012).

261. *See, e.g.*, Benedict Sheey, *Corporations and Social Costs: The Wal-Mart Case Study*, 24 J.L. & COMM. 1, 41 (2004); Michael Farren & Anne Philpot, *With Amazon HQ2, the Losers are the Winners: Why Economic Development Subsidies Hurt More than They Help*, MERCATUS CTR. (2018).

262. *See* RICK WARTZMAN, STILL BROKE: WALMART'S REMARKABLE TRANSFORMATION AND THE LIMITS OF SOCIALLY CONSCIOUS CAPITALISM (2022).

263. *See* Thomas Ross, *The Rhetoric of Poverty: Their Immorality, Our Helplessness*, 79 GEO. L.J. 1499, 1538 (1991) ("Although we acknowledge the existence of tax fraud, we do not see it as so systemic or substantial that it necessitates restructuring the way we implement and monitor our tax system. In contrast, Congress assumes that the welfare system must be implemented and monitored based on the assumption of substantial fraud.").

264. Lipman, *supra* note 142, at 2, 16.

265. *Id.* at 16 (noting that the tax gap is more than the amount spent on income security programs).

266. *Id.* ("[S]ince 1995, real GDP has increased by 76 percent and IRS staffing has decreased by 32 percent. While Congress cut the IRS' budget across all areas, the largest budget cuts have been in IRS enforcement.").

267. NEWSTROM & BLOCK, *supra* note 56, at 4.

percent commit securities fraud, at a cost of $830 billion in destroyed equity value.[268]

Corporate fraud is notably rife in privatized welfare programs.[269] In 2007, Texas cancelled its $899 million contract with Accenture to make welfare eligibility determinations after applications piled up, call centers ignored callers, and eligible people were denied benefits. Nevertheless, Accenture sold its services in other states, and Texas signed other contracts with Accenture to manage Medicaid claims processing and child support payments.[270] A company called Maximus became a major player in welfare privatization, particularly after welfare reform in 1996. In state after state, it failed to deliver on contract terms, harming needy people in the process, and yet states continued to award it contracts at escalating prices. In both Wisconsin and New York, there were conflicts of interest in which Maximus hired family and friends of government officials, while officials threw extra money at the company.[271] Maximus also engaged in profligate spending with taxpayer money, using money to pay for advertising, staff parties, and sales pitches in other states.[272] After Maximus settled a federal prosecution for filing false Medicaid claims, it nevertheless won numerous additional contracts — ironically, to fight Medicaid fraud.[273]

In sum, outsourcing has not increased efficiency and effectiveness in public benefits programs. Rather, it has allowed for rampant profiteering and conflicts of interest by companies.[274] The hypocrisy is stark: "Today, California welfare recipients can be charged with a felony crime for receiving as little as $400 in undue benefits, while

---

268. Alexander Dyck, Adair Morse & Luigi Zingales, *How Pervasive is Corporate Fraud?*, 29 REV. ACCT. STUD. 736 (2024), https://link.springer.com/article/10.1007/s11142-022-09738-5#Sec9 [https://perma.cc/DQC3-49U4]. The authors adopt the SEC definition of fraud as involving misrepresentation, or "to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading." *Id.* at 739.

269. *See* DISCIPLINING THE POOR, *supra* note 133, at 183–84.

270. *See* Aman Batheja, *In State Contracting, Failure is an Option*, TEX. TRIB. (Feb. 1, 2015, at 06:00 CT), https://www.texastribune.org/2015/02/01/cost-overruns-and-bungles-state-contracting/ [https://perma.cc/RZC4-KNLQ] ("Texas' highest-profile disasters [in state contracting] have coincided largely with hulking information technology projects that come in over budget, behind schedule or both.").

271. *See* DISCIPLINING THE POOR, *supra* note 133, at 184–85. Maximus engaged in pay-to-play schemes in several states involving numerous safety net programs and was part of a revolving door between government and private contractors. *See* DANIEL L. HATCHER, THE POVERTY INDUSTRY: THE EXPLOITATION OF AMERICA'S MOST VULNERABLE CITIZENS 38, 40–41 (2016).

272. In Wisconsin alone, "Maximus had spent $51,000 to pay employees seeking new contracts in other states, $196,000 on advertising to promote the Maximus brand, $15,741 on a staff party at an expensive resort, more than $23,000 to hire singer Melba Moore and a group of clowns to entertain corporate clients and staff, and $23,637 for corporate promotional items such as fanny packs and golf balls." DISCIPLINING THE POOR, *supra* note 133, at 184.

273. HATCHER, *supra* note 271, at 29–30 (2016).

274. DISCIPLINING THE POOR, *supra* note 133, at 185.

corporate provider scandals that cost the public millions of dollars produce no criminal charges whatsoever."[275] The poor are criminalized while corporations profit.

IV. SURVEILLANCE CAPITALISM AND THE DATAFIED STATE

Today's growing market in fraud detection algorithms extends the history of racialized welfare surveillance and places it within the grip of surveillance capitalism and the datafied state. The "datafied state" is a way of conceptualizing how the government is using technology to carry out its functions, and in so doing, transforming bureaucracies and citizen-state relations.[276] The state's use of data to manage poor people is not new; it "is more evolution than revolution."[277] The welfare state arose in the 19th Century as a response to people who could not meet their basic needs under capitalism and industrialization.[278] To carry out its social protection programs, the state sought to count and classify its people, their needs, and its available resources,[279] all under the specter of "punitive, moralistic views of poverty."[280]

In the 1980s, widespread computerization served the state's neoliberal drive toward efficiency and cost savings, as governments used technology to implement austerity policies and the criminalization of poverty.[281] With more sophisticated modern technologies, increasing amounts of discretionary authority have moved from bureaucrats to automated systems.[282] At the same time, citizen interactions with the state have shifted from street-level bureaucrats to screen-level systems,[283]

---

275. *Id.*

276. Burell & Singh, *supra* note 20, at 19.

277. EUBANKS, *supra* note 7, at 37.

278. *See* MICHAEL B. KATZ, IN THE SHADOW OF THE POORHOUSE 3–10 (1986).

279. *See* Georgia van Toorn, Chris O'Neill, Maitreya Shah & Mark Andrejevic, *Automation*, *in* KEYWORDS, *supra* note 20, at 106, 109; Lina Dencik & Anne Kaun, *Datafication and the Welfare State*, 1 GLOB. PERSPS. 1 (2020), https://www.diva-portal.org/smash/get/diva2:1448242/FULLTEXT02.pdf [https://perma.cc/D9PT-K7X9]; Paul Henman, *Digital Social Policy: Past, Present, Future*, 51 J. SOC. POL'Y 535, 537–38 (2022), https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A043789F278AA6DBE085E47848877DDF/S0047279422000162a.pdf/div-class-title-digital-social-policy-past-present-future-div.pdf [https://perma.cc/S372-VFCY]; Georgia van Toorn, Paul Henman & Karen Soldatić, *Introduction to the Digital Welfare State: Contestations, Considerations and Entanglements*, 60 J. SOCIO. 507 (2024), https://journals.sagepub.com/doi/epub/10.1177/14407833241260890 [https://perma.cc/L2WG-BWJC].

280. EUBANKS, *supra* note 7, at 16.

281. *See* Burcu Baykurt, *Corporate Capture*, *in* KEYWORDS, *supra* note 20, at 48, 52; EUBANKS, *supra* note 7, at 33–34.

282. *See Automation*, *in* KEYWORDS, *supra* note 20, at 109 ("Initially, digital technologies, and more recently, big data analytics have expanded the state's surveillance capabilities, giving it unprecedented power to monitor and influence a vast range of activities, from communication and movement patterns to financial transactions and the use of government services.").

283. *See* van Toorn, Henman & Soldatić, *supra* note 279.

making it harder for citizens to identify, understand, or challenge adverse decisions.[284] The sorting of the deserving from the undeserving, which is a key project of the welfare state, is now digitized.[285] Identifying fraud has always been a preoccupation of the state, and not surprisingly, it has been subjected to technological transformation.

In the datafied state, the public and private sectors "link up together in deeper alignment."[286] Governments regulate technology but also procure technology from private vendors to carry out their work. Data brokers harvest public data to fuel their profiling, and governments turn around and purchase those very profiles from data brokers, along with other datasets.[287] Thus, the datafied state relies upon surveillance capitalism to carry out its work, while surveillance capitalism profits from public data and its contracts with government agencies.

Under surveillance capitalism, as articulated by Shoshana Zuboff, Big Tech "claims human experience as free raw material for translation into behavioral data," which in turn is used to "shape[] human behavior to others' ends" for profit.[288] The owners of "the new means of behavioral modification" are now the "fountainhead of capitalist wealth and power in the twenty-first century."[289] Zuboff warns that people are losing the "human expectation of sovereignty over one's own life and authorship of one's own experience,"[290] and yet there is "no exit from processes that bypass individual awareness and on which we must depend on for effective daily life."[291] Without individual autonomy, the foundations of a democratic society are destroyed.[292] Meanwhile, surveillance capitalists are "protected by the inherent illegibility of the automated processes that they rule, the ignorance that these processes breed, and the sense of inevitability that they foster."[293]

Zuboff provides an important description of how networked technologies — initially seen as utopian, inherently moral, and

284. *See* Citron, *supra* note 26.

285. *See* Dencik & Kaun, *supra* note 279, at 1; EUBANKS, *supra* note 7, at 16.

286. *Introduction*, *in* KEYWORDS, *supra* note 20, at 25.

287. *See* Matthew Tokson, *Government Purchases of Private Data*, 59 WAKE FOREST L. REV. 269, 273 (2024); Anne Toomey McKenna, *US Agencies Buy Vast Quantities of Personal Information on the Open Market — A Legal Scholar Explains Why and What it Means for Privacy in the Age of AI*, CONVERSATION (June 29, 2023, at 08:16 EDT), https://theconversation.com/us-agencies-buy-vast-quantities-of-personal-information-on-the-open-market-a-legal-scholar-explains-why-and-what-it-means-for-privacy-in-the-age-of-ai-207707 [https://perma.cc/BB9W-E3N3]; Urbana Reviglio, *The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview*, 11 INTERNET POL'Y REV. 1, 2, 6 (2022). Governments at all levels also exchange data, creating an "intergovernmental marketplace." Bridget Fahey, *Data Federalism*, 135 HARV. L. REV. 1007, 1009 (2022).

288. ZUBOFF, *supra* note 19, at 8.

289. *Id.* at 11.

290. *Id.* at 521.

291. *Id.* at 8.

292. *See id*. at 11.

293. *Id.* at 10.

democratizing — have instead become tools for manipulation and corporate domination.[294] However, Zuboff focuses almost exclusively on corporate extraction of data, and thus overlooks the intertwined nature of public and private data sharing and abuses, which manifest in fraud detection algorithms. Further, Zuboff implicitly envisions a White, middle-class consumer as the object of surveillance capitalism, failing to acknowledge how people experience networked technologies differently based on their own identities and positionality.[295]

In light of these gaps, Yeshimabeit Milner from Data for Black Lives and Amy Traub from Demos have developed the theory of data capitalism, which is "an economic model built on the extraction and commodification of data and the use of big data and algorithms as tools to concentrate and consolidate power in ways that dramatically increase inequality along lines of race, class, gender, and disability."[296] Their conception highlights how the underpinnings of surveillance capitalism hinge on racial capitalism, or the ways that capitalism was built on and reinforces racial hierarchies. Within data capitalism, "racial inequality is a feature, not a bug."[297] Milner and Traub emphasize that the power imbalances wrought by data capitalism are not the inevitable result of technological progress but are derived from policy choices.[298]

Indeed, the United States has adopted a policy of allowing markets in personal data to flourish unchecked. At all hours of the day and night, corporations and government are gathering, aggregating, analyzing, and selling people's data.[299] Data is scraped from people's internet activity, social media, app usage, public records, geolocation tracking,

---

294. *See id.* at 9.

295. *See* Sareeta Amrute, *Sounding the Flat Alarm (Review of Shoshana Zuboff, The Age of Surveillance Capitalism)*, B2O (Jan. 27, 2020), https://www.boundary2.org/2020/01/sareeta-amrute-sounding-the-flat-alarm-review-of-shoshana-zuboff-the-age-of-surveillance-capitalism/ [https://perma.cc/WAL6-MPJN] ("The populations that are most at risk under surveillance capitalism include immigrants, minorities, and workers, both within and outside the United States."); Evgeny Morozov, *Capitalism's New Clothes*, BAFFLER (Feb. 4, 2019), https://thebaffler.com/latest/capitalisms-new-clothes-morozov [https://perma.cc/7KRJ-HDTA] ("In Zuboff's telling, it also appears that surveillance capitalism hurts everyone equally. And yet, aren't the retirees of Oslo, whose pensions are — via Norway's sovereign wealth fund — invested in the stocks of surveillance capitalists, predisposed to like it more than the landless workers of São Paulo?").

296. YESHIMABEIT MILNER & AMY TRAUB, DATA FOR BLACK LIVES & DEMOS, DATA CAPITALISM + ALGORITHMIC RACISM 4 (2021).

297. *Id.*

298. *Id.*

299. *See* SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 355–57 (2018); 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-youriphone-is-talking [https://perma.cc/3JZE-AV4Z]; WOLFIE CHRISTL, CRACKED LABS, CORPORATE SURVEILLANCE IN EVERYDAY LIFE 4–19 (2017), https://crackedlabs.org/en/corporate-surveillance [https://perma.cc/U8TT-3JE2].

purchase history, and more.[300] We emit a digital trail with "every search, click, and like, with every tap of our credit card, every search of our map, and every trip to the shops."[301] Data brokers combine our digital exhaust into individualized profiles, which they sell to multiple purchasers, including marketers, law enforcement, financial companies, employers, and government agencies, who then use the profiles for their own purposes.[302] At the same time, these entities are analyzing their own customer and citizen data troves, and then selling that information, thereby creating interconnected networks of data flows.[303] The aggregation of data allows "third parties to know individuals in a way that would be impossible if the information remained dispersed."[304]

All of this happens without the informed consent or knowledge of the people whose data is gathered. To the contrary, "We routinely give away information about ourselves to a wide range of organizations and we have little sense of how we might reclaim that data."[305] While companies value this data for advertising and even the shaping of consumer behavior, marketing is merely the tip of the big data iceberg. Algorithmic decision-making increasingly serves as the gatekeeper to life's necessities, such as housing, employment, health care, financial services, education — and of course, public benefits.[306] Poor people and minorities are on the losing end of these sorting systems. As a result of these algorithmic systems, they are excluded from life's opportunities; they are targeted for subprime goods and services; they are exploited for profit; and they are surveilled at higher rates in their homes, schools, neighborhoods, and workplaces.[307]

---

300. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, 11–14 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-calltransparency-accountability-report-federal-trade-commission-may2014/140527databrokerreport.pdf [https://perma.cc/BY66-56VQ]; Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cellphone.html [https://perma.cc/5YDZ-WU6G] (reporting on the ease of matching billions of location data points originating from a single data location company to specific individuals).

301. Jane Andrew, Max Baker & Casey Huang, *Data Breaches in the Age of Surveillance Capitalism: Do Disclosures Have a New Role to Play?*, 90 CRITICAL PERSPS. ON ACCT. (2023), https://www.sciencedirect.com/science/article/pii/S1045235421001155 [https://perma.cc/RV66-76DQ].

302. FRY, *supra* note 108, at 32; FED. TRADE COMM'N, *supra* note 300.

303. *See* CHRISTL, *supra* note 299.

304. BRIDGES, *supra* note 13, at 136.

305. Andrew et al., *supra* note 301.

306. *See* MICHELE GILMAN, DATA & SOC'Y RSCH. INST., POVERTY LAWGORITHMS: A POVERTY LAWYER'S GUIDE TO FIGHTING AUTOMATED DECISION-MAKING HARMS ON LOW-INCOME COMMUNITIES 1, 10–11 (2020), https://datasociety.net/library/poverty-lawgorithms [https://perma.cc/ZA8L-VZ3V].

307. Michele E. Gilman, *Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice*, 52 AZ. STATE L.J. 368, 371–72 (2020).

Low-income people have more of their data floating through the algorithmic ecosystem, because their data is collected as they access public benefits and live in highly policed neighborhoods. In turn, this data is used to justify increased surveillance and puts them at higher risk of identity theft and misuse of their data.[308] At the societal level, as Ngozi Okidegbe explains, democracy is undermined when states adopt automated systems that deny people a voice in algorithmic uses and construction, and ultimately "suppress the political power of oppressed people in governance."[309] When people are criminalized for welfare fraud, they are politically disempowered, as they can lose voting rights, be cut off from mainstream economic opportunities and social supports, and lose faith in government.[310]

Technology is accelerating the lengthy history of "data and information systems [used] to subjugate and control" in service of an extreme power asymmetry that benefits corporations[311] with minimal transparency or accountability for the harms inflicted disproportionally on low-income people and minorities. The fraud-first presumption that underlies these algorithms is built upon gendered and racist notions of poor people and extends welfare surveillance into the digital age.

V. LAW AND FRAUD DETECTION ALGORITHMS

Computer scientists frame concerns and evaluate solutions for socio-technical systems around the values of fairness, transparency, and accountability.[312] Similar values animate administrative law, which governs how agencies carry out the work delegated to them by legislatures and how courts review that work.[313] These are not just technocratic values. They serve to enhance the dignity of individuals in their relationship with the state, while also supporting the legitimacy of the state.[314] Yet the datafied state is undermining these values, and

308. *See* EUBANKS, *supra* note 7, at 7 (noting that marginalized groups are "singled out for punitive public policy and more intense surveillance, and the cycle begins again").

309. Ngozi Okidegbe, *To Democratize Algorithms*, 69 UCLA L. REV. 1688, 1705 (2023).

310. *Id.* at 1712.

311. MILNER & TRAUB, *supra* note 296, at 6.

312. *See* Donghee Shin & Yong Jin Park, *Role of Fairness, Accountability, and Transparency in Algorithmic Affordance*, 98 COMPUTS. HUM. BEHAV. 277, 277 (2019).

313. David Freeman Engstrom & Daniel E. Ho, *Artificially Intelligent Government: A Review and Agenda*, *in* RESEARCH HANDBOOK ON BIG DATA LAW 57, 60 (Roland Vogl ed., 2021), https://www.elgaronline.com/edcollchap/edcoll/9781788972819/9781788972819.00009.xml [https://perma.cc/A9Y3-LZQ8] ("On the one hand, the body of law that governs how government agencies do their work is premised on transparency, accountability, and reason-giving.").

314. *See* Mike Gregory, *Deciding with Dignity: Automated Decision-Making, the Rule of Law and Procedural Disrespect*, 38 RATIO JURIS 172, 180, 187 (2025) ("[M]uch of the literature on algorithmic governance has focused on transparency, auditability, and outcome

surveillance capitalism remains largely unregulated. As a result, fraud detection algorithms are disproportionately harming minorities and low-income people, while lining the pockets of large corporations and serving the political interests of government in advancing a neoliberal agenda. This Part analyzes how law is failing to uphold the technological and administrative values of fairness, accountability, and transparency. Fraud detection algorithms not only undermine the values of administrative law, but they also fail to prevent the very fraud they were implemented to address.

A. Fairness

The case studies of MiDAS, the Dutch child benefits scandal, and the Australian robodebt debacle reveal two major ways in which benefits fraud algorithms can be unfair:[315] first, they are biased against minorities, and second, they have high error rates resulting in innocent people being accused of fraud. This Section assesses the legal remedies for both forms of unfairness, finding them inadequate.

1. Discrimination

There is ample evidence that predictive fraud algorithms can be biased against minority groups, meaning they generate "outcomes which are systematically less favorable to individuals within a particular group and where there is no relevant difference between groups that justifies such harms."[316] To be sure, algorithms can appear objective compared to human decision-making,[317] which is notoriously infected with conscious and unconscious stereotypes. Indeed, there is well-documented evidence of bias and discrimination in the administration of "analog" public benefits systems. A study by the Urban Institute found

---

fairness . . . . But the procedural rule of law . . . demands . . . that the decision-making process itself be intelligible as a shared exercise in normative reasoning."); Jeremy Waldron, *The Rule of Law and the Importance of Procedure*, *in* NOMOS L: GETTING TO THE RULE OF LAW 3, 6 (James E. Fleming ed., 2011) (noting that the procedural rule of law promotes the dignity of people as capable of explaining themselves).

315. Defining fairness is algorithmic systems is challenging because "[t]he concept of fairness can be used in several ways and can refer to many different normative ideas." Deborah Hellman, *Measuring Algorithmic Fairness*, 106 VA. L. REV. 811, 834 (2020) (reviewing "conceptual distinction[s]" in defining fairness). Hellman also explains why algorithms may need to be race-conscious in order to prevent discrimination, and that such an approach is legal. *Id.* at 846–64.

316. Nicol Turner Lee, Paul Resnick & Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS (May 22, 2019, at 09:45 ET), https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ [https://perma.cc/8KWN-MFXL].

317. *See* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 65 (2019) ("The dominant perception is that algorithms are but simple mathematical principles, rearranged to reveal patterns and make predictions.").

that 11.2 percent and 6.7 percent of low-income Black and Latinx recipients of social service benefits, respectively, reported unfair treatment compared to 3.7 percent of low-income White recipients.[318] Avoiding this sort of discrimination is part of the allure of adopting automated systems.

Unfortunately, discrimination does not disappear when states automate social service delivery. Biased policies become encoded in algorithms, which can reflect the biases of the individuals who design them.[319] Developers exercise human judgment at numerous points while developing an algorithm.[320] Bias can seep into an algorithmic system at any stage. Of particular concern is that algorithms learn to make decisions from training data, which can import historical or structural bias into the outputs.[321] For instance, predictive policing algorithms designed to predict criminal hot spots are fed data about past crimes, and because minority and low-income communities are heavily policed, prior arrest data feeds a self-reinforcing cycle.[322]

Removing data about race and other protected characteristics does not solve this problem because other factors can stand in as proxies, such as zip codes. In addition, the training data may be over- or under-inclusive of certain groups, leading to biased outcomes.[323] Consider facial recognition technologies, which were trained primarily on faces of

---

318. Eleanor Pratt & Heather Hahn, *What Happens When People Face Unfair Treatment or Judgment When Applying for Public Assistance or Social Services?*, URB. INST. (2021), https://www.urban.org/sites/default/files/publication/104566/what-happens-when-people-face-unfair-treatment-or-judgment-when-applying-for-public-assistance-or-social-services_0.pdf [https://perma.cc/JVJ9-XAJG]. Similarly, a Virginia study found that eligibility caseworkers were less likely to be helpful to Black than White recipients as well as less likely to suggest education or training opportunities to them. *See* Rachel Avi Silberman Holtzman, *Emotions Matter: Emotional Distress Damages for Discrimination in Public Benefits*, 3 N.C. CIV. RTS. L. REV. 171, 187 (2023). Within the TANF program nationwide, Black recipients are "significantly more likely" to be sanctioned than White recipients, and higher sanction rates also hold true for other minorities, including recipients who are Hispanic or members of indigenous groups. *Id.* at 185–86.

319. Katyal, *supra* note 317, at 59.

320. *See* Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 ADMIN. L. REV. 1, 15 (2019) ("Human analysts exert substantial control over myriad aspects of an algorithm's functioning."). Developers determine and define an algorithm's goals and desired outputs; identify, collect, and clean the data that feeds the models; select and apply an algorithmic model; screen results for errors and outliers and tweak the model accordingly; set the acceptable levels of false negatives and false positives; and interpret a model's outcomes. *See* David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 672–702 (2017).

321. Pauline T. Kim, *Manipulating Opportunity*, 106 VA. L. REV. 867, 869–70 (2020) ("Predictive algorithms are built by observing past patterns of behavior, and one of the enduring patterns in American economic life is the unequal distribution of opportunities along the lines of race, gender, and other personal characteristics.").

322. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORN. L. REV. 547, 570–71 (2017); Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218, 2253 (2019) ("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.").

323. *See* Katyal, *supra* note 317, at 69–73, 80.

White men, and then resulted in high error rates for women of color.[324] Bias can also manifest when designers frame the problem the algorithm is solving. For instance, how is fraud defined? Does it include unintentional mistakes? What factors are indicative of possible fraud? How is a determination of fraud made?[325] Resolving these questions can reflect societal biases.[326] Notably, the people who design algorithms are not representative of the larger population, and thus they can lack context for their decisions.[327]

A journalistic investigation by *Wired* and *Lighthouse Reports* provided an under-the-hood look at predictive welfare fraud detection algorithms.[328] Using freedom of information laws, the researchers obtained rare access to a machine learning algorithm and the data used to train it in Rotterdam, a city in the Netherlands, which, as noted above, has been rocked by several scandals involving benefits fraud algorithms.[329] Built by Accenture, the algorithm was used by Rotterdam from 2017 to 2021 to identify fraud in benefits programs serving 30,000 people.[330] The investigation found that the algorithm discriminated on the basis of ethnicity and gender.[331]

---

324. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCS. MACH. LEARNING RSCH. 77, 84 (2018).

325. *See* Sina Fazelpour & David Danks, *Algorithmic Bias: Senses, Sources, Solutions*, 16(8) PHIL. COMPASS 1, 2 (2021), https://compass.onlinelibrary.wiley.com/doi/pdf/10.1111/phc3.12760 [https://perma.cc/63F7-SSRP] (using the example of defining student success to illustrate sources of algorithmic bias).

326. Algorithmic bias can also result from how the outputs are deployed in the real world, as users may misinterpret the output or apply it outside of its intended context. *See* David Danks & Alex John London, *Algorithmic Bias in Autonomous Systems*, 26 PROCS. INT'L JOINT CONF. ON A.I. 4691, 4694 (2017).

327. *See* Sara Harrison, *Five Years of Tech Diversity Reports — and Little Progress*, WIRED (Oct. 1, 2019, at 07:00 ET), https://www.wired.com/story/five-years-tech-diversity-reports-little-progress [https://perma.cc/HF4F-R8A8]; Johnson, *supra* note 111, at 1225–27 (explaining the need for diversity in leadership positions for companies that develop and adopt automated decision-making platforms); SARAH MYERS WEST, MEREDITH WHITTAKER & KATE CRAWFORD, AI NOW INST., DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI 6 (2019), https://ainowinstitute.org/discriminatingsystems.pdf [https://perma.cc/A4BD-68K2] ("Currently, large scale AI systems are developed almost exclusively in a handful of technology companies and a small set of elite university laboratories, spaces that in the West tend to be extremely White, affluent, technically oriented, and male."); MEREDITH BROUSSARD, MORE THAN A GLITCH: CONFRONTING RACE, GENDER, AND ABILITY BIAS IN TECH 7 (2023) (noting that this is a more likely cause for algorithmic bias than intentional discrimination).

328. Eva Constantaras, Gabriel Beiger, Justin Casimir Braun, Dhruv Mehtotra & Htat Aung, *Inside the Suspicion Machine*, WIRED (Mar. 6, 2023, at 07:00 ET), https://www.wired.com/story/welfare-state-algorithms/ [https://perma.cc/4TXU-W3XB].

329. *Id.* ("Rotterdam isn't the only city using algorithms to interrogate welfare recipients. But it is, to date, the most transparent about what it's doing. Rotterdam was chosen for this story not because its system is especially novel, but because out of dozens of cities we contacted, it was the only one willing to share the code behind its algorithm.").

330. *Id.*

331. *Id.*

The algorithm was trained on data about people who had been previously investigated for fraud. However, this dataset was flawed, such as being generated from inadequate sample sizes. Further, the researchers found that the algorithm equated honest mistakes as probative of fraud, even though the city itself knew that various reporting requirements were so complex that mistakes were common. Based on this flawed data, the algorithm used 315 variables to assign risk scores to individuals deemed likely to commit fraud. The algorithm combined risk factors with subjective assessments by social workers regarding attributes such as a claimant's appearance and attitude.[332] "The data fed into the algorithm ranges from invasive (the length of someone's last romantic relationship) and subjective (someone's ability to convince and influence others) to banal (how many times someone has emailed the city) and seemingly irrelevant (whether someone plays sports)."[333] Single mothers were tagged as particularly risky. In addition, while the algorithm did not include race or ethnicity among its variables, other input data served as proxies for these factors, such as a data point for non-native Dutch speakers.[334] The city's own internal evaluation documents found that the algorithm performed no better than random selection, and in 2021, Rotterdam suspended use of the algorithm.

Another example of known bias in benefits fraud detection algorithms involves the Earned Income Tax Credit ("EITC") program in the United States. The EITC is a tax credit for low-income workers that lifts over four million Americans out of poverty.[335] It carries less of a social stigma than other social welfare programs due to its connection with work and its delivery as a tax refund rather than a cash benefit.[336] Nevertheless, alleged fraud in the program is a popular punching bag for conservative politicians calling to restrict or reduce the EITC. EITC recipients are audited at twice the rate of the rest of the population, even though the tax gap is driven primarily by high-income White households that underreport income.[337] Of this group, Black taxpayers are

---

332. *Id.*

333. *Id.* ("While the machine learning algorithm used in Rotterdam's system, called a gradient boosting machine, relied on complex mathematics to uncover [hidden] patterns, its basic building block" was 500 decision trees that "categorize individuals based on a series of yes-no questions.").

334. *Id.* ("If someone is rated as struggling with Dutch . . . they are two times more likely to be flagged for a welfare fraud investigation than somebody who is fluent in Dutch.").

335. *Policy Basics: The Earned Income Tax Credit*, CTR. ON BUDGET & POL'Y PRIORITIES (April 28, 2023), https://www.cbpp.org/research/policy-basics-the-earned-income-tax-credit [https://perma.cc/372S-S3BK].

336. *See* Jennifer Sykes, Katrin Križ, Katheryn Edin & Sarah Halpern-Meekin, *Dignity and Dreams: What the Earned Income Tax Credit (EITC) Means to Low-Income Families*, 80 AM. SOCIO. REV. 243, 244 (2014).

337. Lipman, *supra* note 142, at 1, 2–3, 10 ("Most notably, the audit rates of corporations and high-income individuals have dropped precipitously. Audits on millionaires have plummeted 71 percent and on large corporations they have dropped 51 percent.").

audited at about three to five times that of non-Black taxpayers.[338] Although the IRS does not use racial data in its audit selection methods, its machine learning models emphasize factors that are correlated with race, such as underreported income, rather than focusing on less racially correlated factors, such as the extent of underreporting.[339] Black taxpayers are thus targeted for audits despite no evidence that they commit fraud at higher rates than anyone else.[340] The study's authors concluded, "Our results highlight how seemingly technocratic choices about algorithmic design can embed important policy values and trade-offs."[341]

Despite these known biases in algorithms, challenging discriminatory fraud detection algorithms in the United States faces significant hurdles. At the constitutional level, the Equal Protection Clause forbids the federal and state governments from treating individuals or groups differently without sufficient justification.[342] However, it protects against only intentional discrimination.[343] It does not protect against disparate impact discrimination, or the discriminatory outcomes that result from neutral policies and practices. Intent is also required for private actions under Title VI, the federal statute forbidding discrimination in federally assisted programs, which covers most public benefits programs due to their joint federal-state funding

338. HADI ELZAYN, EVELYN SMITH, THOMAS HERTZ, ARUN RAMEST, JACOB GOLDIN, DANIEL E. HO ET AL., STAN. INST. FOR ECON. POL'Y RSCH. MEASURING AND MITIGATING RACIAL DISPARITIES IN TAX AUDITS, 3 (2023), https://assets.law360news.com/1571000/1571386/23-02.pdf [https://perma.cc/KQ7S-2EA3].

339. *See id.* at 5 ("[T]he taxpayers with the highest under-reported taxes tend to be non-Black, but the available data allow the classifier model to assign the highest probabilities of underreporting to more Black than non-Black taxpayers."); Tim Shaw, *Analysis: How the Tax World Has Responded to Stanford's Study on Black Audit Rates*, THOMSON REUTERS (Aug. 3, 2023), https://tax.thomsonreuters.com/news/analysis-how-the-tax-world-has-responded-to-stanfords-study-on-black-audit-rates/ [https://perma.cc/5JHY-HKNF] ("In other words, the IRS favors auditing the highest amount [of] taxpayers they think, intentionally or unintentionally, overstated tax benefit claims rather than recouping the most uncollected tax possible.").

340. *See* Jacob Bogage, *IRS Audits Black Taxpayers More Often Than Other Groups, Agency Confirms*, WASH. POST (May 16, 2023), https://www.washingtonpost.com/business/2023/05/15/tax-audits-black-americans/ [https://perma.cc/7MDU-DVSR] (reporting that the IRS confirmed the Stanford researchers' findings).

341. ELZAYN ET AL., *supra* note 338, at 6. The authors explain that the choice of "label," or the "definition of the outcome being predicted" can "replicate or exacerbate biases." *Id.* at 7.

342. U.S. CONST. AMENDS. V, XIV. The Fifth Amendment extends the Equal Protection Clause to the federal government. The level of scrutiny a court applies in considering the government's justification depends on the alleged basis of discrimination.

343. *See* Washington v. Davis, 426 U.S. 229, 240 (1976) ("[T]he invidious quality of a law claimed to be racially discriminatory must ultimately be traced to a racially discriminatory purpose."); Aziz Z. Huq, *What Is Discriminatory Intent?*, 103 CORN. L. REV. 1211, 1212 (2019) ("'Discriminatory intent' is a central term in the judicial interpretation of constitutional clauses requiring the equal treatment of persons without regard to their race, ethnicity, or religion. There is nothing inevitable about this.").

structures.[344] The intent standard makes it hard to succeed on constitutional or statutory discrimination claims involving fraud detection algorithms. As Andrew Selbst and Solon Barocas explain, most algorithmic discrimination is unintentional.[345] As they note, there is little incentive for a person or entity with conscious bias to expend the cost and effort of designing a discriminatory algorithm when they could easily discriminate without the cover of an algorithm and likely escape liability.[346]

The concept of "intent" under constitutional and statutory law is generally a narrow one.[347] The clearest case of intentional discrimination would be an algorithm designed to disfavor a particular group. A harder, but more common, case involves a defendant who does not set out to discriminate, but also does nothing to prevent it.[348] To be sure, a broader definition of intent "could include knowledge or substantial certainty of the result."[349] Many scholars have argued that courts should impute tort standards into discrimination law (particularly with regard to employment) such that a defendant's negligence or reckless indifference to preventing discrimination would establish discriminatory intent.[350] These proposals are ripe for the algorithmic age, in which

344. Alexander v. Sandoval, 532 U.S. 275 (2001) (holding that intentional discrimination is required to recover under Title VI); *see also* Olatunde C.A. Johnson, *Lawyering That Has No Name: Title VI and the Meaning of Private Enforcement*, 66 STAN. L. REV. 1293, 1305 (2014) ("[T]he Court's core holding seems to render Title VI a procedure for terminating funds or encouraging voluntary compliance with norms determined solely by reference to the Court's constitutional rulings.").

345. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 693 (2016); *see also* Andrés Páez, *Negligent Algorithmic Discrimination*, 84 L. & CONTEMP. PROBS. 19, 26 (2021) ("Many of the decisions involved in training an algorithm are the result of the trainer's implicit prejudices, which in turn may be a reflection of cultural stereotypes prevalent in his social environment. Most discrimination that arises in data mining is thus unintentional."); Aziz Z. Huq, *Constitutional Rights in the Machine-Learning State*, 105 CORN. L. REV. 1875, 1922 (2020) ("[I] am unaware of any instance in which animus on the part of an instrument's designers has been credibly alleged. Discrimination challenges by racial or ethnic minorities based on intent rather than classification, moreover, are notoriously difficult to prove or win.").

346. Barocas & Selbst, *supra* note 345, at 693; *see also Páez*, *supra* note 345, at 25 ("In brief, there is a significant burden of proof placed on the job candidate and the data reflects this burden: Plaintiffs in disparate impact cases only had on average a 19.2 percent success rate in the seven years between 1984 and 2001 for Court of Appeals decisions, and a 25.1 percent success rate in the six years between 1983 and 2002 for District Court decisions.").

347. *See* Stephanie Bornstein, *Reckless Discrimination*, 105 CALIF. L. REV. 1055, 1059 (2017).

348. *See* Katie Eyer, *The But-For Theory of Anti-Discrimination Law*, 107 VA. L. REV. 1621, 1623 (2021) ("Does disparate treatment law in fact prohibit all 'disparate treatment,' (i.e., all decisions in which the outcome would have been different 'but for' race, sex, or other protected class status)? Or does it prohibit only the narrower category of 'intentional discrimination' (i.e., decisions in which protected class status played a conscious role)?").

349. Barocas & Selbst, *supra* note 345, at 700–01.

350. Bornstein, *supra* note 347, at 1061–72 (summarizing proposals). With regard to algorithms used in employment, Ifeoma Ajunwa argues for adoption of a discrimination per se

multiple parties often play a role in developing an algorithmic tool, making a search for a single "intent" fruitless. Moreover, given the widespread evidence of bias in algorithms, it is fair to say that at this point, ignoring the possibility of discrimination is a form of assent.[351]

Indeed, the Consumer Financial Protection Bureau ("CFPB") under the Biden Administration signaled that designers of financial lending algorithms should search for less discriminatory alternatives as part of their fair lending compliance testing.[352] This obligation reflected current knowledge that any algorithm has the potential to discriminate without adequate scrutiny even without intent to do so.[353] However, the Trump Administration issued a rule eliminating disparate impact from ECOA.[354] Thus, while a broader conception of intent is well-suited for algorithmic design, it is not yet the law.[355] The intent requirement also stymies legal redress under administrative law because federal courts do not apply the Administrative Procedure Act's guarantee of non-arbitrariness to claims of racial or ethnic discrimination.[356]

The above analysis is somewhat speculative because thus far, there are no American court decisions involving a welfare benefits algorithm challenged under anti-discrimination law. Accordingly, looking abroad can be informative. In the fraud detection systems scrutinized in the Netherlands, the courts applied anti-discrimination norms embodied in human rights and privacy law. In striking down the SyRI fraud

---

theory, in which an employer's failure to audit its algorithms would establish a prima facie intent to discriminate. Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671, 1733 (2020).

351. *See* Páez, *supra* note 345, at 29 ("In a sense, discrimination has become foreseeable by default, thus making these systems intrinsically harmful.").

352. Brad Blower, *CFPB Puts Lenders & FinTechs On Notice: Their Models Must Search For Less Discriminatory Alternatives Or Face Fair Lending Non-Compliance Risk*, NAT'L CMTY. REINVESTMENT COAL. (Apr. 5, 2023), https://ncrc.org/cfpb-puts-lenders-fintechs-on-notice-their-models-must-search-for-less-discriminatory-alternatives-or-face-fair-lending-non-compliance-risk/ [https://perma.cc/L8G5-WPDZ].

353. *See* Exec. Order No. 14,281, 90 Fed. Reg. 17537 (Apr. 23, 2025) (stating the disparate impact theory of discriminatory intent is unconstitutional and directing federal agencies to align with the new policy). On the dismantling of the CFPB, *see* Laurel Wamsley, *New CFPB Chief Closes Headquarters, Tells All Staff They Must Not Do 'Any Work Tasks'*, NPR (Feb. 10, 2025, at 10:47 ET), https://www.npr.org/2025/02/08/nx-s1-5290914/russell-vought-cfpb-doge-access-musk [https://perma.cc/X2V3-B5D3].

354. Equal Credit Opportunity Act (Regulation B), 91 Fed. Reg. 21620 (Apr. 22, 2026).

355. *See* Bornstein, *supra* note 347, at 1072 ("[F]ederal courts appear loathe to recognize that an employer entity has an affirmative duty to prevent, a responsibility to correct, or even an obligation not to perpetuate such bias."). Selbst and Barocas argue that the FTC can regulate discriminatory AI products and services through its "unfair and deceptive acts and practices" authority. *See* Andrew D. Selbst & Solon Barocas, *Unfair Artificial Intelligence: How FTC Intervention can Overcome the Limitations of Discrimination Law*, 171 U. PA. L. REV. 1023, 1024–25 (2023).

356. *See* Cristina Isabel Ceballos, David Freeman Engstrom & Daniel E. Ho, *Disparate Limbo: How Administrative Law Erased Antidiscrimination*, 131 YALE L.J. 370, 370, 415–24 (2021) (describing how courts avoid applying APA § 704 by finding "adequate remedy" through other actions).

detection algorithm, the reviewing court found that the algorithm was unlawful based on Article 8 of the European Convention on Human Rights, which protects everyone's "right to respect for his private and family life, his home and his correspondence."[357] The court stated that these privacy rights included rights to equal treatment and protection against discrimination.[358] The risk model used in SyRI could result in unintentional discrimination against immigrants or people with lower socio-economic status because it was deployed only in "problem neighbourhoods."[359] By comparison, in the United States, unintentional discrimination in a public benefits program would not trigger constitutional or statutory protections.

Similarly, in the childcare benefits scandal, the Dutch Data Protection Authority found that the Tax Authority discriminated by including nationality as a risk factor in its algorithm. Because nationality had no bearing with regard to benefit eligibility, including it as a factor violated the anti-discrimination protections of the General Data Protection Regulation (or the AVP in Dutch).[360] In a post-mortem of the scandal, Amnesty International pointed out that discriminatory algorithmic design decisions violate various human rights obligations binding in the EU.[361] By contrast, in the United States, we do not have a comprehensive privacy law protecting personal data,[362] and international human rights are not enforceable in our courts.

Currently, the strongest measures against algorithmic discrimination in the United States have come from the executive branch under the Biden Administration, but these are no longer in effect.[363] In 2023,

---

357. Rb.-Haag 5 februari 2020, NJ 2020, 1878 m.nt EJD [*In re* Dutch Jurists Committee for Human Rights v. State of the Netherlands] (Neth.) at 6.21 https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:865 [https://perma.cc/LRP8-8LT4].

358. *Id.* at 6.24.

359. *Id.* at 6.91, 6.93.

360. *Tax Authorities Fine for Discriminatory and Unlawful Practices*, AUTORITEIT PERSOONSGEGEVENS (Dec. 7, 2021), https://autoriteitpersoonsgegevens.nl/actueel/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze [https://perma.cc/TK3M-WFQZ]. Article 9 of the General Data Protection Regulation (EU) 2016/679 ("GDPR") prohibits the processing of personal data revealing characteristics such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation unless there is consent or countervailing public interests.

361. AMNESTY INT'L., *supra* note 78, at 21–23.

362. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 357 NW. L. REV. 357, 370 (2022).

363. A variety of Biden Administration actions on AI were listed at *Administration Actions on AI*, AI.GOV, https://web.archive.org/web/20241221013318/https://ai.gov/actions/ [https://perma.cc/VLF6-SPSG]. Additional White House actions are detailed at *US Federal AI Governance: Laws, Policies and Strategies*, IAPP (June 14, 2023), https://iapp.org/resources/article/us-federal-ai-governance/#white-house [https://perma.cc/3V6X-EVFS].

the Biden Administration issued an Executive Order ("EO") on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence asserting that the administration will not "tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice."[364] The EO required federal agencies that oversee public benefits programs to develop plans to ensure due process, transparency, and anti-discrimination.[365] However, President Trump rescinded the EO.[366] Thus, in the United States, non-discrimination principles tailored for algorithmic systems are subject to executive whim unless they are codified in law and made enforceable.[367]

2. Inaccuracy

Unfairness also arises when algorithmic errors strip people of needed support and wrongfully accuse them of fraud. Although computer-generated outcomes have a veneer of accuracy, they are only as reliable as their human designers. Unfortunately, "[p]rogrammers routinely change the substance of rules when translating them from human language into computer code."[368] For instance, programmers in Colorado inaccurately translated at least nine hundred state regulatory requirements into computer 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 improper denials of food stamps to the disabled.[369] Further, the data fed into an algorithmic system can be faulty. In the MiDAS system for UI, the fraud detection algorithm was churning faulty data, in part due to a failure to transfer data from a legacy system to MiDAS accurately and fully.[370]

In another example, the Social Security Administration in 2018 began using an algorithmic product called Accurint, sold by LexisNexis, to determine whether recipients of Supplemental Security Income (a benefit for the elderly, extremely low-income, and disabled people) had unreported real property that disqualified them from benefits.[371]

---

364. Exec. Order No. 14,110, 3 C.F.R. 657, 658 (2024).

365. *See id.* at 682–83.

366. Exec. Order No. 14,148, 90 Fed. Reg. 8237, 8240 (Jan. 20, 2025).

367. *See* Amos Toh & Ivey Dyson, *The Nuts and Bolts of Enforcing AI Guardrails*, JUST SEC. (May 30, 2024), https://www.justsecurity.org/96201/enforcing-ai-guardrails/ [https://perma.cc/RB6D-RPFH].

368. Citron, *supra* note 26, at 1254.

369. *Id.* at 1256, 1268–69.

370. *See supra* Section II.A.

371. SARAH MANCINI, KATE LANG & CHI CHI WU, NAT'L CONSUMER LAW CTR., MISMATCHED AND MISTAKEN: HOW THE USE OF AN INACCURATE PRIVATE DATABASE RESULTS IN SSI RECIPIENTS UNJUSTLY LOSING BENEFITS 3 (2021), https://www.nclc.org/wp-content/uploads/2022/08/RptMismatchedFINAL041421-1.pdf [https://perma.cc/Y8X3-CN9N].

LexisNexis promoted Accurint as a "powerful tool" for "combating entitlements fraud," used by over 3,000 agencies.[372] Yet legal services advocates across the country soon began finding that their clients were being cut off from benefits or assessed for overpayments based on false accusations of owning disqualifying property.[373] An investigation found that the "matching standards being used in Accurint are shockingly lax," as the system relies solely on a first and last name match.[374] This name matching practice disproportionately impacted people of color, who are more likely to have similar names. For instance, the 2010 Census showed that one quarter of the Hispanic population shares twenty-six surnames.[375] "The upshot of this failure to require any reasonable standard of accuracy is that low-income people are being cut off from minimal subsistence-level benefits due to erroneous real property matches."[376]

Other fraud detection systems are similarly sloppy. In 2024, the Electronic Privacy Information Center ("EPIC") filed a complaint with the Federal Trade Commission ("FTC") alleging unfair and deceptive practices regarding benefits fraud detection systems developed and sold by Thomson Reuters called Fraud Detect and sold in at least forty-two states.[377] Fraud Detect ranks benefits recipients based on their fraud and overpayment risk.[378] It does so by combining public benefits program data with a wide array of consumer data such as criminal background information, housing, and social media information. Yet the algorithm is not accurate.[379] Rather, "Fraud Detect has been used to claw back purported years-old improper overpayments from public benefits recipients who did not commit fraud, falsely flagging consumers as fraudsters when agency officials erred."[380] Out of ten million UI claims paid out by California in the early months of the pandemic, Fraud Detect flagged 1.1 million as suspicious, resulting in suspension of benefits for all those claimants.[381] Yet more than 600,000 of the supposedly fraudulent claims were later cleared as legitimate, for a mere forty-six percent accuracy rate.[382]

---

372. *Id.* at 12.

373. *See id.*

374. *Id.* at 4.

375. *Id.* at 21. After litigation and regulatory supervision, the big three credit reporting agencies have stopped using name only matching. *Id.*

376. *Id.* at 4. A government audit found that seven percent of the Lexis search results resulted in a false match, while only 4.6 percent generated accurate matches that impacted eligibility. *Id.* at 23.

377. *See* EPIC Complaint, *supra* note 122.

378. *Id.* ¶ 52.

379. *Id.* ¶¶ 46–50, 64. These practices also raise the risk of discrimination because criminal background checks and housing information disproportionately disadvantage minorities due to "historical redlining practices and racial disparities in policing." *Id.* ¶ 46.

380. *Id.* ¶ 44.

381. *Id.* ¶ 45.

382. *Id.*

The United States has no comprehensive privacy law giving people rights to control their data, or even to know when their data is being collected and for what purpose. Given congressional gridlock to pass such a law, twenty states have passed their own data privacy laws.[383] While they differ in their consumer-protectiveness, they generally give consumers certain rights to control their data, such as accessing, deleting, and correcting their data, while placing obligations on businesses to effectuate those rights and prevent privacy-related harms.[384] However, these laws typically do not apply to state and local government agencies.[385]

These laws might apply to the private vendors selling fraud detection algorithms to state agencies, although the liability as between algorithmic developers and deployers is often not clear.[386] At least one federal court held in a Fair Housing Act challenge to a tenant screening algorithm that a developer effectively contracted away its liability for the outcomes of its tools.[387] In any event, most benefits claimants have no idea when they are subject to an algorithmic determination and certainly would have no idea where or how to access the data about them held by a particular vendor, which in turn is harvesting data from multiple public and private sources.[388] Even if a claimant could follow the trail to access their personal data, a right of correction of one's personal

383. IAPP, *US State Privacy Legislation Tracker* (Feb. 10, 2026), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/CM4H-FHET]; *see* Aziz Z. Huq, *The Unexpected Robustness of American AI Regulation*, KU LEUVEN (July 23, 2024), https://www.law.kuleuven.be/ai-summerschool/blogpost/the-unexpected-robustness-of-american-ai-regulation [https://perma.cc/DPQ4-JK3N] (discussing how states are taking the lead in AI regulation).

384. IAPP, *US State Privacy Legislation Tracker*, *supra* note 383.

385. *See* JORDAN FRANCIS, FUTURE OF PRIVACY FORUM, ANATOMY OF STATE COMPREHENSIVE PRIVACY LAW: SURVEYING THE STATE PRIVACY LAW LANDSCAPE AND RECENT LEGISLATIVE TRENDS (2024), https://fpf.org/wp-content/uploads/2024/11/REPORT-Anatomy-of-State-Comprehensive-Privacy-Law.pdf [https://perma.cc/M896-QMXF] ("Another category of entities almost universally excluded are government entities. Definitions vary, but government entities usually encompasses any political subdivision of the state."); *see, e.g.*, MD. CODE ANN., COMM. L. § 14-4703(a)(1) (the Maryland Online Data Privacy Act of 2024 does not apply to "[a] regulatory, administrative, advisory, executive, appointive, legislative, judicial body or instrumentality of the State, including a board, bureau, commission, or unit of the State or a political subdivision of the State").

386. *See* Selbst & Barocas, *supra* note 355, at 1032–35 (describing various civil rights laws and whether they would reach algorithmic developers).

387. Connecticut Fair Hous. Ctr. v. CoreLogic Rental Prop. Sols., LLC, 167 F.4th 605, 624 (2d Cir. 2026).

388. *See, e.g.*, LYDIA X. Z. BROWN, MICHELLE RICHARDSON, RIDHI SHETTY, ANDREW CRAWFORD & TIMOTHY HOAGLAND, CTR. FOR DEMOCRACY & TECH., CHALLENGING THE USE OF ALGORITHM-DRIVEN DECISION-MAKING IN BENEFITS DETERMINATIONS AFFECTING PEOPLE WITH DISABILITIES 8 (2020), https://cdt.org/wp-content/uploads/2020/10/2020-10-21-Challenging-the-Use-of-Algorithm-driven-Decision-making-in-Benefits-Determinations-Affecting-People-with-Disabilities.pdf [https://perma.cc/PHH6-92KS] (reviewing challenges to public benefits decisions in which courts found that "people receiving some form of state-funded benefit lost their benefits, either completely or partially, with inadequate notice or no notice at all").

data would not remedy inaccuracies in an algorithm's coding or the numerous other ways that algorithms can lead to incorrect results. Nor do individual rights to correction push an agency to make determinations about the acceptable levels of false positives and negatives or other fairness tradeoffs, which would require agencies to make complex policy judgments, ideally in consultation with a range of stakeholders.[389]

On paper, consumer law provides some limited avenues for relief. The FTC could enforce its jurisdiction to remedy unfair and deceptive acts or practices through Section 5 of the FTC Act.[390] While the Act does not apply to state agencies, it does apply to the private vendors that sell their tools to state governments.[391] The argument is that fraud detection algorithms are injuring public benefits claimants with inaccurate and arbitrary fraud determinations; that consumers are unable to avoid these harms due to the lack of transparency of these systems; and that the countervailing benefits of fraud detection do not outweigh the harms.[392] The FTC could, and should, examine the fraud detection systems sold by private venders, particularly those already linked to systemic failures. Still, the FTC alone is not sufficient to combat the spread of these systems as the resources of the FTC are limited, with a small staff devoted to privacy enforcement,[393] and currently, an administration unfriendly to consumers. Moreover, the FTC cannot fine companies unless they violate an existing consent order, and fines have been

389. *See* Hellman, *supra* note 315, at 828 ("The fact that we cannot have both equal predictive value and error rate balance in most circumstances leads to the question: which should we prefer and why?"). The COMPAS algorithm used to predict recidivism risk in bail determinations raised this issue starkly. In a ground-breaking investigation, ProPublica showed that COMPAS had unequal error rates across racial groups — Black defendants were more likely to be false positives while White defendants were more likely to be false negatives — violating equalized odds, even though the vendor argued the tool was calibrated, meaning a given risk score predicted the same reoffending probability for everyone. *See* SOLON BAROCAS, MORITZ HARDT & ARVIND NARAYANAN, FAIRNESS AND MACHINE LEARNING: LIMITATIONS AND OPPORTUNITIES 74, 97 (2023). Because base rates of reoffending differed across groups, COMPAS could not simultaneously satisfy both calibration and equalized odds, forcing a choice between fairness definitions, of which there are many. *Id.* at 98–100. Ngozi Okidegbe argues that impacted populations should have a meaningful say in these value determinations. Ngozi Okidegbe, *To Democratize Algorithms*, 69 UCLA L. REV. 1688, 1697–98 (2023).

390. 15 U.S.C. § 45(a). An unfair act or practice is one which "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). *See* Luke Herrine, *Unfairness Reconstructed*, 42 YALE J.L. & REG. 95, 103–05, 126–37 (2025) (discussing the history of FTC's "unfairness" enforcement actions and its expansive and vigorous enforcement under the Biden administration's FTC).

391. EPIC Complaint, *supra* note 122, ¶ 53 ("The Commission has stated that a company also violates Section 5 of the FTC Act when it furnishes others with the means and instrumentalities for the commission of unfair and deceptive acts and practices.").

392. *Id.* ¶¶ 51, 64, 78.

393. *See* 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, at 06:48 ET), https://theconversation.com/74-screens-of-legalese-dont-protect-your-data-heres-a-blue [https://perma.cc/L9KC-44CZ].

"small in relation to the gravity of the violations."[394] Meanwhile, private parties cannot enforce the FTC Act.

By contrast, private parties, as well as the FTC and the CFPB, can enforce the Fair Credit Reporting Act ("FCRA"), which was enacted in 1970 to promote the accuracy, fairness, and privacy of personal information gathered by consumer reporting agencies ("CRAs").[395] A CRA includes a company that compiles information used to establish a consumer's financial eligibility for a government benefit.[396] CRAs must "follow reasonable procedures to assure maximum possible accuracy" in consumer reports,[397] and the FCRA gives consumers the right to dispute accuracy in a consumer report,[398] with obligations on the CRA to timely investigate those disputes.[399] Yet the vendors of fraud detection algorithms have claimed they are not CRAs and that fraud detection is not a credit related purpose.[400] Even if vendors lose these arguments,[401] the FCRA's statutory promise has not translated to the real world even for clearly covered entities. For instance, credit reporting mistakes are a widespread and longstanding phenomenon, persisting despite the FCRA.[402] Federal enforcement of the FCRA is limited due to resource

394. Daniel J. Solove & Woodrow Hartzog, *FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 605 (2014).

395. 15 U.S.C. §§ 1681–1681x. CRAs are entities that assemble and generate consumer reports, which contain information "bearing on a consumer's . . . character, general reputation, personal characteristics, or mode of living." *Id.* §§ 1681m(a)–(b).

396. *Id.* § 1681b(a)(3)(D) (providing that a CRA is "required by law to consider an applicant's financial responsibility or status").

397. *Id.* § 1681e(b).

398. *Id.* § 1681b(b)(3)(B)(IV).

399. *Id.* § 1681i(a)(1)(A).

400. *See* Lauren Bikoff, *Trade Groups Stress the Importance of Fraud Detection Amid FCRA Rulemaking*, WOLTERS KLUWER (June 25, 2024), https://www.vitallaw.com/news/fair-credit-reporting-trade-groups-stress-the-importance-of-fraud-detection-amid-fcra-rulemaking/blw0120b16f5640d34b969e03c3aa1da48d0b [https://perma.cc/PTY3-PR6P]; *see also* Chi Chi Wu, *Data Gatherers Evading the FCRA May Find Themselves Still in Hot Water*, NAT'L CONSUMER L. CTR. (June 14, 2019), https://library.nclc.org/article/data-gatherers-evading-fcra-may-find-themselves-still-hot-water [https://perma.cc/6ZWU-J32U] (discussing whether data brokers are covered by the FCRA and noting that "three circuit courts this year have shown a reluctance to respect the FCRA's plain language and its expansive coverage").

401. If they are covered entities, they could be liable for violating the FCRA, such as by including prohibited information in reports (such as old civil and criminal judgments), failing to ensure maximum accuracy of the reported information, withholding information from state agencies thus making it impossible for claimants to see the basis for a fraud alert or high risk score, or failing to reinvestigate upon a consumer dispute. *See* EPIC Complaint, *supra* note 122, ¶¶ 83–87.

402. 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-percentconsumers-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, 308 (2016).

constraints.[403] Private enforcement faces numerous hurdles, ranging from lack of transparency about algorithmic systems, the costs of bringing lawsuits combined with negligible damages, and numerous procedural barriers.[404]

Another approach is to challenge inaccurate and arbitrary fraud detection algorithms under the Constitution, which requires reasoned decision-making by government as a matter of due process. Although the Court has refused to recognize a substantive constitutional right to welfare, the landmark 1970 case of *Goldberg v. Kelly* established that welfare benefits were a form of property and thus could not be terminated without the due process protections of prior notice and a hearing.[405] Even before government automation, due process was a mixed revolution when it comes to public benefits. While it has provided low-income people with an essential forum to assert their rights, its shortcomings include a lack of lawyers to enforce those rights, an adversarial rather than problem-solving approach, an often demeaning and confusing process, and a masking of systemic injustice through the framework of individual fair hearings.[406] In the algorithmic context, these concerns are magnified due to the lack of explanation, even in the setting of a live hearing. Hearings are meaningless without effective confrontation of black box systems and when decision-makers are infected with

---

403. *See* FED. TRADE COMM'N, FAIR CREDIT REPORTING ACT, EFFORTS TO PROMOTE CONSUMER REPORT ACCURACY AND DISPUTES, A REPORT TO CONGRESS 4–6 (2020), https://www.ftc.gov/system/files/documents/reports/fair-credit-reporting-act-efforts-promote-consumer-report-accuracy-disputes-report-congress/ftc_disputes_and_accuracy_report_2020_corrected_version.pdf [https://perma.cc/FVU3-XPTE]. The CFPB also enforces the Fair Credit Reporting Act. *Id.* at 4.

404. *See* Austin H. Krist, Note, *Large-Scale Enforcement of the Fair Credit Reporting Act and the Role of State Attorneys General*, 115 COLUM. L. REV. 2311, 2318 (2015) (noting that the consumer recourse process under the FCRA has been described as a "Kafkaesque no man's land."). With regard to litigation barriers, see *id.* at 2319–23. One judge, in regretfully dismissing a case, commented that the FCRA was not only "hopelessly complex," but also "includes numerous provisions that limit consumers' ability to enforce its mandates either by explicitly barring private actions or by imposing such burdensome procedural requirements that no layperson could possibly be expected to comply." Burrell v. DFS Servs., 753 F. Supp. 2d 438, 444 (D.N.J. 2010). *See generally* Alexandra P. Everhart Sickler, *The (Un)Fair Credit Reporting Act*, 28 LOY. CONSUMER L. REV. 238, 241 (2016) (observing that the "[FCRA] is a hybrid private-public enforcement regime that is not cohesive and has created regulatory voids.").

405. 397 U.S. 254, 267 (1970).

406. *See* Jason Parkin, *Adaptable Due Process*, 160 U. PA. L. REV. 1309, 1331 (2012) (summarizing critiques of fair hearing rights, including that "[f]air hearings do not address barriers that prevent eligible individuals from applying for welfare in the first instance"); Rebecca E. Zietlow, *Giving Substance to Process: Countering the Due Process Counterrevolution*, 75 DENVER U. L. REV. 9, 26 (1997) ("[F]ormal procedural rights may hurt rather than help poor people because they serve to mask substantive injustice."); Michael Herz, *Parallel Universes: NEPA Lessons for the New Property*, 93 COLUM. L. REV. 1668, 1710 (1993) (stating that due process in public benefits regimes has "contributed to routinization, alienation, and abuse").

automation bias (the tendency to rely upon automated outputs over human judgment).

Not surprisingly, scholars are split on the utility of individualized hearings in the context of algorithmic decision-making. Due process claims have had mixed success in litigation challenging automated public benefits systems, including fraud detection systems.[407] Several of the cases challenging MiDAS involved due process claims. In the *Cahoo* case, after years of litigation, class certification was denied and only four individual plaintiffs remained.[408] The plaintiffs settled claims against the private contractors,[409] while the court ultimately dismissed claims against the state officials on the basis of qualified immunity, reasoning that they did not violate clearly established due process rights because the fraud determinations created "collection issues for prior payments, not a termination of current benefits."[410] Plaintiffs in other class actions against MiDAS that settled waited almost a decade for compensation.[411]

This lengthy, expensive process to vindicate due process rights is par for the course in challenges to algorithms. Most claimants are unrepresented and as a result, many of those people waive their rights to a hearing.[412] Those who manage to find legal representation rely on under-resourced legal aid offices who must triage numerous other cases

---

407. *See* RASHIDA RICHARDSON, JASON M. SCHULZ & VINCENT M. SOUTHERLAND, LITIGATING ALGORITHMS 2019 US REPORT: NEW CHALLENGES TO GOVERNMENT USE OF ALGORITHMIC DECISION SYSTEMS, AI NOW INSTITUTE 19–23 (2019), https://ainowinstitute.org/wp-content/uploads/2023/04/litigatingalgorithms-2019-us.pdf [https://perma.cc/F39N-B68F] (describing litigation against automated public benefits systems).

408. Cahoo v. Fast Enters., 508 F. Supp. 3d 138, 144 (E.D. Mich. 2020).

409. Adrienne Roberts, *Claimants Falsely Accused of Michigan Unemployment Fraud Settle with Vendors for $180K*, DETROIT FREE PRESS (Jan. 24, 2024, at 16:45 ET), https://www.freep.com/story/money/business/michigan/2024/01/24/michigan-unemployment-fraud-lawsuit/72324312007/ [https://perma.cc/2W6F-46LN].

410. Cahoo v. SAS Inst., Inc., 71 F.4th 401, 409 (6th Cir. 2023). The court stated that "the MiDAS program's imperfections indeed are many . . . . It does not make sense to empower a computer program to make fraud findings, even for internal purposes, that require assessing a claimant's intent." *Id.* at 411. Nevertheless, these were policy failings and not constitutional ones.

411. *See* Adrienne Roberts, *Michigan Court OKs $55M Settlement in Pandemic-Era Unemployment Benefits Lawsuit*, DETROIT FREE PRESS (May 15, 2025, at 16:16 ET), https://www.freep.com/story/money/business/michigan/2025/05/15/michigan-class-action-lawsuit-unemployment-benefits-jobless/83644158007/ [https://perma.cc/9R5B-SUY4] (reporting on *Saunders* litigation); Beth LeBlanc, *A Decade Later, Michigan Workers Falsely Accused of Fraud Get a Slice of Justice*, DETROIT NEWS (Jan. 29, 2024), https://www.detroitnews.com/story/news/local/michigan/2024/01/29/michigan-unemployment-insurance-agency-false-fraud-hardships-bankruptcy-rick-snyder-settlement-check/72397236007/ [https://perma.cc/J2VG-DFVR] (reporting on settlement in *Bauserman* litigation).

412. *See* COLO. CTR. ON L. & POL'Y, BARRIERS, ERRORS, & DUE PROCESS DENIED: A REVIEW OF COLORADO'S SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM ADMINISTRATIVE HEARING PROCESS 9 (2022) (showing that the national average of claimants waiving their right to a hearing for food stamp fraud is 44.8 percent, while in Colorado, it is 67 percent).

and issues. It is common for cases to bounce up and down the trial and appellate courts while state agencies continue to violate due process.[413] Further, procedural victories to obtain notice, improved explanations, and hearings before human beings have not changed the landscape at the design level.[414] Automated welfare systems continue to strip qualified people of benefits, and there are no ex ante requirements to embed due process or substantive quality norms into the design stage of algorithmic development.

Accordingly, many scholars contend that an individualized remedy cannot fix systemic problems.[415] Danielle Citron argues for a reimagined procedural due process for the automated age, such as through releasing algorithmic source code and training judges on the fallibility of technology.[416] Aziz Huq likewise acknowledges the need for a new due process paradigm, but argues that better algorithmic design on the front end and systemic litigation as necessary on the back end will solve due process deficiencies better than individualized human review.[417] He contends that individual hearing officers are unlikely to identify how "[d]eviations from a tolerably accurate pattern of predictions can result from the design of the training data, the outcome variable selection, or the choice of algorithmic instrument," and are certainly ill-suited to remedy those failings.[418]

Margot Kaminski & Jennifer Urban push back against the undermining of individualized rights, arguing that the individual right to contest both public and private uses of AI is essential to meet due process norms, particularly of human dignity.[419] However, they appear to have an overly rosy view of what actually happens in due process

---

413. *See* RICHARDSON, SCHULTZ & SOUTHERLAND, *supra* note 407, at 7; Soren Dal Rasmussen & Kevin De Liban, *Narrating Justice: Client-Centered Media Advocacy*, SARGENT SHRIVER NAT'L CTR. ON POVERTY L. 2–4 (2018), https://clinical.aals.org/wp-content/uploads/sites/3/2019/05/media_articles.pdf [https://perma.cc/B64P-35DF] (discussing due process lawsuits challenging an Arkansas Medicaid algorithm and state obstruction).

414. *See* RICHARDSON, SCHULTZ & SOUTHERLAND, *supra* note 407, at 19–25 (assessing the success of litigation against automated decision-making systems). A key recommendation of the report is: "Assess the success of litigation by measuring structural change within government agencies and their programs, rather than through isolated or narrow changes to specific ADS." *Id.* at 12. The authors note that litigation itself is not enough to remedy harms, as a "successful . . . strategy must include coalition work . . . ." *Id.*

415. Engstrom & Ho, *supra* note 313, at 14 ("The scholarly literature may be moving away from individual, privately enforced rights as the best way to achieve accountability in favor of 'accountability by design.'").

416. *See* Citron, *supra* note 26, at 1284, 1306.

417. Huq, *supra* note 345, at 1948–49.

418. *Id.* at 1909.

419. Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 1957, 1973 (2021) ("Contestation is a core mechanism for establishing the preserving justice in the Western adversarial tradition.").

hearings.[420] Still, studies on perceptions of fairness in algorithmic systems show that as the human stakes of algorithmic decision-making get higher, people become more concerned about algorithmic governance, which can be tempered by opportunities for contestation.[421] Public perceptions of procedural fairness in decision-making impact the legitimacy of, and compliance with, governmental actions.[422] Moreover, procedural fairness enhances the dignity of people subject to decision-making.[423] For all these reasons, the ability to contest governmental decision-making before a human adjudicator is essential.[424] In short, there is value in the range of conceptions of due process: We need ex ante design requirements that embed fairness and accuracy in algorithmic systems along with individualized ex post hearing rights to enforce these norms.

B. Accountability

Martha Minow describes accountability as "being answerable to authority that can mandate desirable conduct and sanction conduct that breaches identified obligations. In a democracy, the ultimate authority should be the general population . . . ."[425] Automated decision-making systems pose several barriers to accountability. As the case studies show, many of the agencies using fraud detection systems deployed biased and inaccurate systems, failed to provide claimants with explanations of the fraud accusations, did not provide meaningful human review of the algorithmic determinations, and obfuscated system failures. The benefits and shortcomings of due process litigation to guarantee accountability have already been addressed. This Section analyzes the challenge to accountability wrought by privatization.

Fraud detection algorithms are one aspect of privatized poverty governance. Companies claim they will reduce fraud, dependency, and

420. *See* Lucie E. White, *Subordination, Rhetorical Survival Skills, and Sunday Shoes: Notes on the Hearing of Mrs. G.*, 38 BUFF. L. REV. 1, 37 (1990) (describing the dignity-stripping function and effect of public benefits due process hearings).

421. Amit Haim & Dvir Yogev, *What do People Want from Algorithms? Public Perceptions of Algorithms in Government*, 49 L. & HUM. BEHAV. 263, 273–74, 277 (2025) ("Essentially, we suggest that people tend to be more accepting of algorithmic decision making when they feel a greater sense of control and individuation over the process or an opportunity to influence the process.").

422. *Id.* at 264.

423. Gregory, *supra* note 314, at 184.

424. *See infra* Part VI. Strategies for Flipping the Fraud-First Presumption (discussing substituting the fraud-first presumption for support-first presumption).

425. Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229, 1260 (2003).

bureaucratic red tape better than government agencies.[426] Yet privatization shifts policymaking authority to private actors, thereby lessening democratic control over public policies.[427] When governments deliver a service directly, they operate subject to constitutional guarantees, transparency laws, administrative law, and respondeat superior doctrines, among other accountability controls.[428] However, when private companies deliver services on behalf of government, these governance tools do not necessarily follow, even though "the power and responsibility bestowed upon AI vendors to provide the functions of government is increasing dramatically."[429]

Under the state action doctrine, private parties are only liable for constitutional violations if their actions are "fairly attributable" to the state.[430] The application of state action doctrine is a "necessarily fact-bound inquiry."[431] The state action issue was heavily litigated in the one of the MiDAS cases, in which the plaintiffs[432] sued three private companies[433] that developed the system for deprivation of procedural

426. *See* DISCIPLINING THE POOR, *supra* note 133, at 176, 182; Alfred C. Aman & Joseph C. Dugan, *The Human Side of Public-Private Partnerships: From New Deal Regulation to Administrative Law Management*, 102 IOWA L. REV. 883, 908–09 (2017) (describing four stages of the shift from the welfare state towards privatization).

427. *See* Landyn Rookard, *The Common Threats of Artificial Intelligence and Privatization*, 12 TEX. A&M L. REV. 831, 847 (2025) ("That is, rather than taking ownership of policies that may disproportionately impact disadvantaged groups, privatization helps government officials pass policy decisions off as inevitable and objective results of the 'all-knowing' market."); Aman & Dugan, *supra* note 426, at 890; Engstrom & Ho, *supra* note 313, at 4 (noting how humans are being pushed out of the loop); Hannah Bloch-Wehba, *A Public Technology Option*, 86 L. & CONTEMP. PROBS. 223, 224 (2023) ("Efforts to modernize the state reflect the prioritization of innovation over accountability and invite co-optation by the private vendors increasingly responsible for building, maintaining, and managing government technology.").

428. *See* Kimberly N. Brown, *Outsourcing, Data Insourcing, and the Irrelevant Constitution*, 49 GA. L. REV. 607, 634 (2015).

429. Kate Crawford & Jason Schultz, *AI Systems as State Actors*, 119 COLUM. L. REV. 1941, 1958 (2019).

430. Rendell-Baker v. Kohn, 457 U.S. 830, 838 (quoting Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982)) (internal quotation marks omitted).

431. Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 288–89 (2001). To make this determination, courts generally examine whether the private actor is carrying out a public function (public function theory), whether it is entangled with the state in provision of a public service (joint participation theory), or whether the state directs or compels the private party's conduct (compulsion theory). *Id.* at 289, 301, 311.

432. Plaintiffs sought class certification, which was denied, and ultimately there were three individual plaintiffs remaining in the *Cahoo* case. *See* Order Denying Motion to Certify Class at 1, 33, Cahoo v. Fast Enters., No. 17-10657 (E.D. Mich., Dec. 12, 2020) (holding that the alleged due process violations were too different among the putative class).

433. The vendors were CSG Government Solutions ("CSG"), Fast Enterprises ("Fast"), and SAS Institute ("SAS"). CSG, as the consultant procured to manage the system modernization project, was the most involved with UIA operationally and strategically. Fast provided the software and IT architecture which comprised MiDAS. SAS provided a data analytics solution which complemented, but remained distinct from, MiDAS, called the Enterprise Fraud Detection System. Each vendor's contract began at a different time and was procured separately. *Cahoo I*, 322 F. Supp. 3d 772, 787–88 (E.D. Mich. 2018).

due process.[434] In *Cahoo*, the federal district court ruled that several vendors qualified as state actors due to their entanglement with the state.[435] CSG Government Solutions ("CSG") was the company hired to manage the modernization of the UI system. Its entanglement with the state involved joint reporting relationships between government and CSG staff, co-location of employees of both entities, and CSG staff's use of State of Michigan email addresses.[436] With regard to Fast Enterprises ("Fast"), which provided the software and IT architecture for MiDAS, the entanglement involved the State's active supervision and approval of Fast and its deliverables, the training that Fast provided to state staff, Fast's role in drafting the forms and notices which provided legally insufficient notice to claimants, and the responsibility the state delegated to Fast for ensuring compliance with Federal and State law.[437] The case ultimately settled,[438] so the constitutional liability of these companies was never resolved.

Further, these entanglement findings were very fact-specific to the relationship between the MiDAS vendors and the State of Michigan. The entanglement theory makes it unlikely that an off-the-shelf product with less government oversight will qualify as a state actor, even though the risk of harm heightens in that situation. In other words, the more responsibility the government outsources, the less liability it or its vendors will face.[439]

---

434. This was the only claim that survived after multiple motions to dismiss. Cahoo v. Fast Enters., 528 F. Supp. 3d 716, 726 (E.D. Mich. 2021).

435. State action was addressed in *Cahoo I*, 322 F. Supp. 3d 772, 797 (E.D. Mich. 2018), and Cahoo v. Fast Enters. LLC, 580 F. Supp. 3d 494, 499 (E.D. Mich. 2022) [hereinafter *Cahoo IV*]. In *Cahoo IV*, the court found that discovery had borne out the thrust of plaintiffs' alleged facts, but by that time, SAS had been dismissed from the suit for lack of personal jurisdiction. *See* Cahoo v. SAS Inst. Inc., 2020 WL 4700822, at *4 (E.D. Mich. 2020). The court observed that, since "SAS's software had nothing to do with adjudicating, denying or terminating benefits, assessing penalties or restitution, collecting wages, intercepting taxes, or handling mail, phone calls, or appeals," that the plaintiffs' injury was not fairly traceable to SAS. *Id.* at *2, *4.

436. 580 F. Supp. 3d at 500.

437. *Id.* at 501–02.

438. Shortly after this decision, CSG and Fast settled with the three remaining *Cahoo* plaintiffs, paying $120K and $60K respectively. *See* Adrienne Roberts, *Claimants Falsely Accused of Michigan Unemployment Fraud Settle with Vendors for $180K*, DETROIT FREE PRESS (Jan. 24, 2024, at 16:45 ET), https://www.freep.com/story/money/business/michigan/2024/01/24/michigan-unemployment-fraud-lawsuit/72324312007/ [https://perma.cc/6ZXY-YGUM].

439. *See* Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1371 (2003) ("Worse still, focusing on government involvement creates perverse incentives for governments to forego close oversight of their private partners, even though such oversight is an important means for ensuring that private actors adhere to constitutional requirements."); *see also* Crawford & Schultz, *supra* note 429, at 1968–70 (arguing for courts to adopt broad and flexible readings of state action in AI vendor cases because government does not understand the tech it is deploying, thus making it essential that courts are able to order relief from the party best situated to fix errors).

State action can also be found when a private entity exercises functions traditionally and exclusively performed by the state.[440] Because private organizations have long supported the poor, and because the government is not required to provide public benefits as a constitutional matter, courts may conclude that a private vendor's AI fraud detection algorithm does not constitute a "traditionally and exclusively" public function.[441] The state action doctrine also provides no restraints on a government's decision to outsource in the first place.[442]

Vendors have disclaimed not only constitutional liability, but also various statutory obligations. With regard to the Accurint[443] algorithm discussed above, LexisNexis claimed that its real property searches did not have to meet the accuracy standards of consumer reporting agencies under the FCRA, and Social Security Administration ("SSA") then used this disavowal to deny claimants the opportunity to contest the agency's findings.[444] In other words, the outsourcing of eligibility determinations allowed the government to freeride on the private vendor's self-serving determination that it did not have to comply with governing law.

As with Accurint and the SSA, sometimes privatization puts the government and its contractors in cahoots against citizens, but privatization can also lead to finger pointing between the state and its contractors when systems fail — leaving citizens in a lurch. In 2006, Indiana awarded a $1.34 billion contract to a consortium of contractors led by IBM to manage its public benefits applications through centralized call centers.[445] There were two primary justifications for outsourcing: to

---

440. *See* Jackson v. Metropolitan Edison Co., 419 U.S. 345, 352 (1974); *see also The Public Function Concept*, 2 TREATISE ON CONST. L. § 16.2 ("[T]he operation of election systems, the governance of cities and towns, and, perhaps, the operation of seemingly public facilities such as parks will be deemed public functions regulated by the Constitution.").

441. Metzger, *supra* note 439, at 1415–16; *cf. In re* Bank of Am. Cal. Unemployment Benefits Litig., 674 F. Supp. 3d 884, 939 (S.D. Cal. 2023). The Bank of America ("BANA") held a contract with California to issue EBT cards to UI claimants. *Id.* at 902. A class of plaintiffs sued the BANA for, inter alia, deprivation of due process when, as a result of fraud, they lost money in their accounts and suffered account freezes, denying them access to their funds. *Id.* at 903–04. On a motion to dismiss, the court rejected BANA's argument that it was not a state actor, ruling that BANA performed a traditionally and exclusively government function because it was "invested with the power to distribute EDD benefits payments, and if it freezes an account, to suspend a claimant's access to those benefits which have already been distributed." *Id.* at 940.

442. *See* Kimberly N. Brown, *We the People, Constitutional Accountability, and Outsourcing Government*, 88 IND. L.J. 1347, 1368 (2013) ("As a means for triggering accountability, however, the test's requirement of coercive state power over the private actor has it exactly backwards: It relieves from constitutional scrutiny altogether those contractors who exercise the *most* discretion pursuant to the *least* amount of government involvement or oversight.").

443. *See supra* text accompanying notes 371–376.

444. *See* MANCINI ET AL., *supra* note 371, at 3, 5.

445. *See* Alfred C. Aman Jr., *Globalization and the Privatization of Welfare Administration in Indiana*, 20 IND. J. GLOB. LEGAL STUD. 377, 394, 397, 399 (2013) (noting that the contract covered SNAP, Medicaid, TANF, and other social assistance programs).

save costs through technology and to reduce mistakes and fraud.[446] The actual "*welfare* of the individuals involved" was not considered.[447] Serious problems soon emerged — the contractor lost documents and its software malfunctioned, while claimants faced lengthy hold times, application processing delays, and wrongful denials of eligibility.[448] At one point, workers were denying applications "just to reduce the backlog."[449] Heartrending stories emerged, such as an eighty-year old woman whose Medicaid benefits were terminated when she was hospitalized for heart failure and thus did not call an eligibility hotline at the required time.[450]

In October 2009, Governor Mitch Daniels pulled the plug on the contract.[451] The state sued IBM for $1.3 billion, and IBM countersued for $52.8 million for its equipment.[452] The state and the contractor traded barbs: The state said that IBM's system was rife with data errors, while IBM blamed rising caseloads due to the recession and natural disasters.[453] A judge overseeing the litigation lamented, "Overall, both parties are to blame and Indiana's taxpayers are left as apparent losers."[454] Ultimately, the Indiana courts ruled that IBM breached the contract and awarded the state $78 million in damages.[455]

As the Indiana debacle shows, due to privatization, claimants can be stuck in an accountability void wrestling with the fallout from faulty systems while the contractor points its fingers at the agency and vice versa. Compounding this accountability void was a contractual clause between the parties denying claimants any rights to enforce the terms of the contracts as third-party beneficiaries.[456] On this issue, the public and private entities ostensibly charged with caring for citizens agreed.

---

446. *See id.* at 388.

447. *Id.* at 388.

448. *See* Aman & Dugan, *supra* note 426, at 909; DISCIPLINING THE POOR, *supra* note 133, at 183.

449. Aman, *supra* note 445, at 411 (quoting Matea Gold, Melanie Mason & Tom Hamburger, *Indiana's Bumpy Road to Privatization*, L.A. TIMES (June 24, 2011)).

450. *See id.* at 410.

451. *See id.* at 413.

452. Rick Callahan, *Appeals Court Affirms Ruling that IBM Owes Indiana $78M*, AP (Sep. 28, 2018, at 17:02 EST), https://apnews.com/general-news-36ba0562a02142e5adfe39518e2e0f85 [https://perma.cc/8RHS-QCJQ]; Andy Opsahl, *IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal*, GOV. TECH. (July 26, 2010), https://www.govtech.com/health/ibm-and-indiana-suing-each-other.html [https://perma.cc/DY5L-XQQ7].

453. Robert N. Charette, *Indiana and IBM Sue Each Other Over Failed Outsourcing Contract*, IEEE SPECTRUM (May 14, 2010), https://spectrum.ieee.org/indiana-and-ibm-sue-each-other-over-failed-outsourcing-contract [https://perma.cc/XE2B-RS3E].

454. Indiana v. Int'l Bus. Machs. Corp., No. 49D10-1005-PL-021451, slip op. at 1 (Marion Super. Ct., Civ. Div. 10, July 18, 2012).

455. *See* Callahan, *supra* note 452.

456. Aman, *supra* note 445, at 387.

C. Transparency

Transparency is "the availability of information about an actor allowing other actors to monitor the workings or performance of this actor."[457] It is essential for accountability. However, there are at least three layers of opacity in algorithmic systems, including those aimed at benefits fraud detection. To begin with, many claimants have no idea that an automated system is responsible for a fraud accusation. Agencies do not publicize their decision to adopt an automated system or seek public input for the decision, even though such a decision can involve a transfer of policymaking authority from the government to the private sector.[458] Robert Brauneis and Ellen Goodman highlight this transparency deficit, stating, "Algorithmic governance has a politics. Judgments are encoded in the algorithmic process at all stages. These are judgments that at some level the public should know and speak to."[459] Yet in the systems at issue in Michigan, the Netherlands, and Australia, the role of automated systems only came to light as increasing numbers of needy people began seeking legal help, calling their representatives, and telling their stories to journalists. It required a torrent of malfeasance followed by years of dogged advocacy to shed light on these systems.[460]

Moreover, it is questionable whether and when the government must provide notice and comment before adopting an algorithmic system. Administrative law requires that before an agency issues a legislative rule with the force of law, it must provide the public with notice of the proposed regulations and an opportunity to provide comment on the proposal.[461] Ideally, notice-and-comment procedures provide the agency with the benefit of multiple perspectives, head off potential harms, and build trust in governmental policies.[462] However, the line between legislative rules that require notice and comment and the other

---

457. Nicholas Diakopoulos, *Transparency*, *in* THE OXFORD HANDBOOK OF ETHICS IN AI 197 (Markus D. Dubber, Frank Pasquale & Sunit Das eds. 2020) (quotation omitted).

458. *See* Hannah Bloch-Wehba, *Transparency's AI Problem*, KNIGHT FIRST AM. INST. (June 17, 2021), https://knightcolumbia.org/content/transparencys-ai-problem [https://perma.cc/ND3X-SZST] ("Automated decision systems are often procured in secret or with limited public oversight."); Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH 103, 109 (2018) ("The risk is that the opacity of the algorithm enables corporate capture of public power.").

459. Brauneis & Goodman, *supra* note 458, at 119.

460. *See supra* Part III.

461. 5 U.S.C. § 553 (2012). States also require notice and comment procedures in their administrative procedure acts. *See* Arthur Earl Bonfield, *The Federal APA and State Administrative Law*, 72 VA. L. REV. 297, 316 (1986).

462. *See* Cass R. Sunstein, *"Practically Binding": General Policy Statements and Notice-and-Comment Rulemaking*, 68 ADMIN. L. REV. 491, 500 (2016). At the same time, "Notice and comment is a protracted process and, when combined with pre-enforcement review, can stymie innovation and prevent dynamic government responses to a changing policy problem or regulatory landscape." Engstrom & Ho, *supra* note 313, at 839.

forms of agency policymaking which do not require notice and comment (e.g., guidance documents, policy statements, procedural rules, and interpretative materials), is not often clear, and case law provides no reliable path through the thicket.[463]

This line is even blurrier when an agency chooses to adopt algorithms for carrying out its decision-making. Is shifting from human to automated decision-making a rule or merely an internal mechanism for carrying out a rule?[464] In the context of determining whether the adoption of algorithms constitutes a legislative rule, commentators have proposed variously that courts look to the degree of human involvement in the decision-making loop, the distributive consequences, whether the algorithm is determinative of outcomes, and/or whether the algorithm creates substantive policy.[465] Yet even if a legislative rule is at issue, it is not clear what aspects of the algorithmic model an agency would have to disclose in its notice to make it meaningful and understandable. Further, there are hard questions about whether any notice could adequately capture the ways in which a model adapts over time.[466]

At least one court has used a notice-and-comment theory to enjoin a welfare benefit eligibility algorithm. In *Arkansas Department of Human Services v. Ledgerwood*,[467] Medicaid recipients challenged an algorithm that allocated caregiver hours to claimants with disabilities.[468] Under the algorithm, which replaced the discretion of registered nurses, claimants lost attendant care hours by an average of forty-three percent. As a result, some claimants went without food or bathing, remained in soiled clothes, missed treatments, had an increased risk of falling, and were isolated in their homes.[469] The Arkansas Supreme Court ruled that the state failed to provide adequate notice and comment of the changes wrought by the algorithmic system.[470] Yet this does not mean the algorithm cannot be used, or that it must meet certain quality standards. It requires only that the agency solicit the statutorily required input — or find a theory to evade notice and comment. Indeed, after the initial program was enjoined, the state issued an emergency rule to use the same

---

463. *See* Engstrom & Ho, *supra* note 313, at 837.

464. *See* Peter Henderson & Mark Krass, *Algorithmic Rulemaking vs. Algorithmic Guidance*, 37 HARV. J.L. & TECH. 105, 107 (2023) (calling this a "doctrinal gray zone").

465. Engstrom & Ho, *supra* note 313, at 836–39 (2020); Amit Haim, *The Administrative State and Artificial Intelligence: Toward an Internal Law of Administrative Algorithms*, 14 U.C. IRVINE L. REV. 103, 127–32 (2024).

466. *See* Haim, *supra* note 465, at 129 ("Agencies could provide global explanations and details over methodology, including data description and model choice, but the model architecture and weights are not suitable for notice-and-comment. This is especially true when such details may adapt over time and releasing them for public comment in every iteration will essentially be a death sentence.").

467. 530 S.W.3d 336 (Ark. 2017).

468. 530 S.W.3d 336, 344–45 (Ark. 2017).

469. *See id.* at 340.

470. *See id.* at 345.

algorithm; the Arkansas Supreme Court upheld the subsequent rule under the emergency rulemaking exception to notice and comment.[471]

Even if a person becomes aware that an automated system is responsible for a fraud accusation, it is likely that both the government and the vendor will claim trade secrecy protection over the inner workings of the algorithm and that open records laws will exempt this information from disclosure.[472] Open records laws were designed to give citizens the right to know what their government is doing.[473] However, these laws were drafted in an era with much stricter demarcations between public and private functions.[474] Thus, litigants have struggled with mixed success to obtain records relating to the privatization of automated decision-making welfare systems.

The Freedom of Information Act ("FOIA") does not require disclosure of information in private hands, and when it comes to algorithmic welfare systems, vendors often retain control over source code, training and input data, and the design and validation processes.[475] Further, government agencies will use their ignorance about the algorithmic systems they purchase as an excuse for failing to prevent harms.[476] For instance, the District of Columbia's Department of Human Services adopted the Thomson Reuters Fraud Detect system, but in response to an open records request, it "revealed that it had no documents pertaining to accuracy testing for the Fraud Detect system, nor any information on how its contract with Thomson Reuters has impacted public benefits recipients within the District of Columbia."[477] Similarly, when Robert Brauneis and Ellen Goodman sent forty-two open records requests to twenty-three states relating to their use of predictive algorithms, most governments did not respond, and those that did often did not have "records concerning the creation and implementation of algorithms."[478]

---

471. *See* Ark. Dep't of Hum. Servs. v. Ledgerwood, 571 S.W.3d 911, 913 (Ark. 2019). The dissent agreed with the circuit court that the emergency rule was "a fabricated and manufactured 'emergency' designed by [the agency] to avoid following the notice and comment requirements [for nonemergency rules] of Arkansas law." *Id.* at 918 (Kemp, J., dissenting).

472. *See* Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1272 (2020) ("These systems frequently come with license agreements, memoranda of understanding, or other documentation evincing claims that the contents are trade secrets.").

473. *See* Aman & Dugan, *supra* note 426, at 924.

474. *See* Alfred C. Aman Jr. & Landyn W. Rookard, *Private Government and the Transparency Deficit*, 71 ADMIN. L. REV. 437, 441 (2019) (footnotes omitted) ("FOIA, especially as originally conceived and drafted, is ill-suited to provide access to privately-created or privately-held information — regardless of the public nature, importance, or funding of the information. FOIA's structure, at present, reflects the unyielding and imprecise private-public dichotomy."); Bloch-Wehba, *supra* note 458, at 6.

475. *See* Bloch-Wehba, *supra* note 458, at 8 ("In many cases, the vendor of an algorithmic system that is licensed to the government will continue to 'control' the source code for the tool, leaving it outside of FOIA's reach."); Brauneis & Goodman, *supra* note 458, at 135.

476. *See* Brauneis & Goodman, *supra* note 458, at 109, 116–17.

477. EPIC Complaint, *supra* note 122, at ¶ 52.

478. Brauneis & Goodman, *supra* note 458, at 109, 151–52.

In addition to its limited scope, FOIA and many of its state counterparts exempt trade secrets from disclosure.[479] When challenged, vendors claim trade secrecy protections over their algorithms, and they include non-disclosure terms in their government contracts to keep agencies silent.[480] Accordingly, scholars have proposed that government agencies should contract for transparency when they procure automated welfare systems by demanding a waiver of trade secrecy protections and insistence on control over all relevant aspects of the algorithmic system.[481] Given the self-interest that government agencies may have in obscuring algorithmic systems from public view, such procurement policies for transparency may need to be legislatively mandated.

Yet even if the trade secrecy hurdle is overcome, there remains a challenge in understanding how an algorithm arrived at a particular outcome, such as a fraud determination. A human decision-maker may be biased, but the legal system can demand that they explain the basis for their decision.[482] By contrast, algorithmic systems based on machine learning have been called black boxes, meaning "they discern patterns and make predictions in a way that cannot be intuitively understood or explained in the same way a conventional analysis can be."[483] Full disclosure can "result in an unmanageable deluge of information, making it very difficult, if not impossible, for the public to understand how data are used and how intelligent platforms generate outcomes."[484] Government officials (and certainly most claimants) often lack technical literacy to understand the systems they deploy or to decode system

479. *See* Bloch-Wehba, *supra* note 472, at 1300 ("FOIA's broad exemption for trade secrets and confidential business information was intended to stimulate information sharing with the government, not to shield government decision-making from public scrutiny.").

480. *See* Bloch-Wehba, *supra* note 458, at 8, 13.

481. *Id.* at 17 (footnote omitted) ("At a bare minimum, statutes should limit agencies' ability to enter into vendor contracts that purport to circumvent open records obligations. As a matter of public policy — and as a matter of transparency law — the prevalent practice of contracting for secrecy is questionable at best."); Elizabeth A. Rowe & Nyja Prior, *Procuring Algorithmic Transparency*, 74 ALA. L. REV. 303, 308 (2022) (arguing that procurement law can alleviate transparency concerns in algorithmic contracting); Cary Coglianese & Erik Lampmann, *Contracting for Algorithmic Accountability*, 6 ADMIN. L. REV. ACCORD 175, 180 (2021) (describing the advantages of a contracting approach as "highly actionable and adaptable").

482. *See* Reuben Binns, Max Van Kleek, Michael Veale, Ulrik Lyngs, Jun Zhao & Nigel Shadbolt, *"It's Reducing a Human Being to a Percentage"; Perceptions of Justice in Algorithmic Decisions*, CHI '18, at 1 (2018).

483. Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 ADMIN. L. REV. 1, 14 (2019); *see also* PASQUALE *supra* note 25, at 3 (2016) (characterizing the "black box" problem as one in which "we can observe its inputs and outputs, but we cannot tell how one becomes the other").

484. Peter K. Yu, *Beyond Transparency and Accountability: Three Additional Features Algorithm Designers Should Build into Intelligent Platforms*, 13 NE. U. L. REV. 263, 277 (2021).

outputs.[485] When government officials adopt algorithmic recommendations that they neither understand nor can explain, "[t]he government has lost democratic accountability, the public cannot assess the efficacy and fairness of the governmental process, and the government agent has lost competence to do the public's work in any kind of critical fashion."[486] A lack of explainability undermines citizen trust in government.[487]

Due to complex machine learning processes, sometimes an algorithm's designers cannot even explain how the system arrives at a given outcome.[488] "[M]achine learning outputs are often nonintuitive in that the rules they derive to make predictions are so complex, multi-faceted, and interrelated that they defy practical inspection, do not comport with any practical human belief about how the world works, or simply lie beyond human-scale reasoning."[489] Thus, giving a claimant the source code underlying an algorithm will not necessarily provide meaningful transparency to advance accountability.[490]

As a result, some commentators urge default use of interpretable models rather than complex machine learning models.[491] Yet this approach faces the headwinds of corporate interest. As Cynthia Rudin points out, businesses make money from developing complicated algorithms, rarely face the consequences of their systems, and thus have little interest in developing models that would be less complex and thereby less proprietary.[492] In short, companies profit from opacity.

---

485. *See* Brauneis & Goodman, *supra* note 458, at 131 (stating that "transparency does not necessarily render an algorithm 'interpretable.'"); *see also* Engstrom & Ho, *supra* note 313, at 64 ("Capacity-building, in short, is central to realizing algorithmic governance's promise *and* avoiding its perils.").

486. Brauneis & Goodman, *supra* note 458, at 109.

487. *See* Stephan Grimmelikhuijsen, *Explaining Why the Computer Says No: Algorithmic Transparency Affects the Perceived Trustworthiness of Automated Decision-Making*, 83 PUB. ADMIN. REV. 241, 253 (2022).

488. *See* Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 BERKELEY TECH. L.J. 773, 788 (2019) (explaining that the black box phenomenon can happen due to the "inability of humans, even those who design and deploy machine learning systems, to understand the dynamic models learned by complex machine learning systems"); Coglianese & Lehr, *supra* note 483, at 16 ("Machine-learning algorithms are deemed 'black boxes' because it is difficult to put into intuitive language how they function.").

489. Engstrom & Ho, *supra* note 313, at 59–60.

490. *See id.* at 61.

491. *See* Boris Babic & I. Glenn Cohen, *The Algorithmic Explainability "Bait and Switch,"* 108 MINN. L. REV. 857, 908 (2023); Cynthia Rudin, *Stop Explaining Black Box Models for High Stakes Decisions and Use Interpretable Models Instead*, 1 NATURE MACH. INTELL. 206, 206 (2019).

492. *See id.* at 209; *see also* JACOB WARD, THE LOOP: HOW TECHNOLOGY IS CREATING A WORLD WITHOUT CHOICES AND HOW TO FIGHT BACK 138 (2022) (noting that opacity helps companies evade liability because black boxes make it difficult to identify cause and effect).

D. Real Fraud

Just as law is struggling to provide adequate recourse to the falsely accused, it is failing to rein in criminals committing real fraud by stealing from public benefits systems. During the pandemic, stealing UI benefits was easy due to the surveillance capitalist networks that market personal data. Criminals set out to file bulk claims in multiple states.[493] They appropriated the Social Security Numbers of dead and incarcerated people to file claims.[494] They gathered personal information from phishing emails by posing as health agencies, such as the Centers for Disease Control and the World Health Organization, and from pharming, or the mimicking of UI agency websites.[495] Criminals nabbed identities exposed in data breaches — between 2010 and 2019, there were at least 2,229 data breaches, exposing nearly 6.9 billion records.[496] Agency insiders accessed their employers' databases and stole customers' personal information to file fake claims.[497]

A ProPublica investigation found that criminal syndicates in China and West Africa hired low-wage teams to churn out fake claims.[498] Communities of fraudsters gathered on messaging apps to trade tips on how to file bogus claims, along with state-specific instructions on evading security checks.[499] According to the investigation, "Some of the forums have thousands of participants and regularly offer stolen identities for sale, alongside tech tips, screenshots that ostensibly prove the methods work and advice on which states are easiest to game and which are 'lit' — that is, still paying out fake claims."[500] Today, criminals are

493. *See* PANDEMIC RESPONSE ACCOUNTABILITY COMM., WHY UNEMPLOYMENT INSURANCE FRAUD SURGED DURING THE PANDEMIC 6 (2024).

494. *See* Richard Lardner, Jennifer McDermott & Aaron Kessler, *The Great Grift: How Billions in COVID-19 Relief was Stolen or Wasted*, AP (June 12, 2023, at 00:01 ET), https://apnews.com/article/pandemic-fraud-waste-billions-small-business-labor-fb1d9a9eb24857efbe4611344311ae78 [https://perma.cc/JJT8-PY8Z].

495. *See* PANDEMIC RESPONSE ACCOUNTABILITY COMM., *supra* note 493, at 6; MICHAEL LEVI & RUSSELL G. SMITH, AUSTRALIAN INST. OF CRIMINOLOGY, FRAUD AND ITS RELATIONSHIP TO PANDEMICS AND ECONOMIC CRISES: FROM SPANISH FLU TO COVID-19 21 (2021).

496. *Data Breaches*, PRIV. RTS. CLEARINGHOUSE, https://privacyrights.org/data-breaches [https://perma.cc/9J33-FLFH].

497. *See, e.g.*, PANDEMIC RESPONSE ACCOUNTABILITY COMM., *supra* note 493, at 2 ("The largest fraud case we reviewed was a fraud ring near Atlanta, Georgia, which involved eight different co-conspirators and over $30 million dollars in stolen UI benefits. In this case, a healthcare worker who had access to patients' personally identifiable information ('PII') sold this information to other co-conspirators who then used the stolen identities to file for pandemic UI benefits.").

498. *See* Cezary Podkul, *How Unemployment Insurance Fraud Exploded During the Pandemic*, PROPUBLICA (July 26, 2021, at 05:00 ET), https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic [https://perma.cc/5C67-JCUC].

499. *See id*.

500. *Id.*

keeping up with the generative AI trend; a website called FraudGPT advertises its ability to "create malicious computer code, write scam letters and hack websites."[501]

Massive troves of consumer data may be exposed in data breaches, making it easy for thieves to steal personal data and fraudulently obtain welfare benefits. Law has not reduced these thefts or significantly reformed corporate behavior to improve cybersecurity; to the contrary, the rate of data breaches continues to increase.[502] While all fifty states have laws requiring companies to notify people whose personal data has been breached,[503] and some also require notification to state regulators, these laws have not significantly shaped corporate behavior. As Woodrow Hartzog and Daniel Solove explain, these laws do not cure the harm; they just inform people of the danger.[504] While companies may suffer a reputational hit or a drop in stock prices after a data breach,[505] they lack adequate incentives to invest in cybersecurity measures because they do not have to bear the full costs of a breach, which are passed on to victims.[506]

Further, when identity theft victims sue companies who hold their data, courts often hold that they lack standing unless they can identify a specific, concrete harm.[507] For many courts, emotional distress, risk of harm, and spending time and money to prevent fraud do not qualify as sufficient harms for standing purposes.[508] Further, identifying harm

---

501. *See* McKenzie Funk, *What a Leading State Auditor Says About Fraud, Government Misspending and Building Public Trust*, PROPUBLICA (June 14, 2024, at 06:00 ET), https://www.propublica.org/article/how-remote-work-ai-impact-fraud-local-government [https://perma.cc/P2QU-UNFT]. *See also* LANA SWARTZ, ALICE E. MARWICK & KATE LARSON, SCAMGPT: GENAI AND THE AUTOMATION OF FRAUD: A PRIMER, DATA & SOCIETY 5 (2026), https://datasociety.net/wp-content/uploads/2025/05/ScamGPT-GenAI-and-the-Automation-of-Fraud_final.pdf [https://perma.cc/FW4H-WQ2M] ("Generative AI exacerbates existing scam tactics by expanding scale, accelerating speed, and increasing efficiency. The technology serves as an intensifier and force multiplier for scams, broadening their reach and impact.").

502. WOODROW HARTZOG & DANIEL SOLOVE, BREACHED!: WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 9 (2022).

503. *See* Aniket Kesari, *Do Data Breach Notification Laws Work?*, 26 N.Y.U. J. LEGIS. & PUB. POL'Y 173, 175 (2023).

504. HARTZOG & SOLOVE, *supra* note 502, at 7.

505. *See id.* at 4; Muhammed Zia Hydari, Yangfan Liang & Rahul Telang, Sound and Fury, Signifying Nothing? Impact of Data Breach Disclosure Laws (June 20, 2024) (unpublished paper), https://arxiv.org/html/2406.15215v1 [https://perma.cc/A2EJ-ZZZV] (finding no evidence of a decline in revenue following a massive data breach at retailer Home Depot).

506. *See* Sangchul Park, *Why Information Security Law Has Been Ineffective in Addressing Security Vulnerabilities: Evidence from California Data Breach Notifications and Relevant Court and Government Records*, 58 INTL. REV. L. & ECON. 132, 132–33 (2019); Tracy C. Miller, *Navigating Data Security Challenges: Policy Innovations and Reform Options*, MERCATUS RSCH. 1, 3 (2024) ("This can be blamed on the fact that in many cases for firms, the cost of a data breach is small relative to the cost of preventing it.").

507. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 740 (2018).

508. *See* HARTZOG & SOLOVE, *supra* note 502, at 56–58 (noting that courts are divided on the nature of sufficient harms).

can be difficult for victims who do not know how their data is being used or do not find out for many years.[509] Indeed, victims who learn that their identity has been used to apply for public benefits constitute almost one-third of identity theft reports, but these discoveries often happen months or years after a breach.[510] Even where harms are known and concrete, it can be difficult to trace the harm to a specific breach at a specific company.[511] In addition, identity theft disproportionately harms low-income people who have the least resources to pursue remedies.[512] Criminal lawsuits against identity thieves are no deterrent because these thieves easily avoid detection; indeed, only one percent of identity theft crimes result in a conviction.[513]

Some states have enacted a variety of cybersecurity laws imposing "reasonable" practices or specific standards on companies,[514] and yet cyberattacks are also increasing over time, in part because they "are not always immediately visible and attribution is challenging even over time."[515] Many companies ignore these laws, and enforcement is often no more than a "slap on the wrist."[516] The FTC is empowered to bring lawsuits for inadequate security practices under the FTC Act's Section 5 prohibitions on unfair and deceptive practices, and the agency has brought dozens of cases against companies who allegedly lied about their security practices in their privacy policies (deceptive) or failed to reasonably safeguard personal data (unfair).[517] However, in 2018, the Eleventh Circuit vacated an FTC cease-and-desist order, holding that it was too vague in its demand for reasonable data security standards.[518] And, in 2021, the Supreme Court held that the FTC cannot seek monetary damages, further limiting the FTC's efficacy.[519] Jeff Kosseff summarizes the state of affairs thusly: "[T]he patchwork of U.S. statutes and regulations that constitute cybersecurity is an uncoordinated mishmash of requirements that mostly were conceived long before modern cyberthreats."[520] In short, technology makes real fraud frictionless to commit, while law offers no counterweight.

---

509. For instance, after a Veterans Affairs Medical Center breach, the court found no cognizable harms for victims from "lost time, anxiety, the increased risk of fraud they faced, their lost privacy over their personal and health information, and their expenditure of money to protect themselves." *Id.* at 35–37.

510. *See* Kesari, *supra* note 503, at 180.

511. *See* HARTZOG & SOLOVE, *supra* note 502, at 59.

512. *See* Sara S. Green, *Stealing (Identity) from the Poor*, 106 MINN. L. REV. 59, 65 (2021).

513. *See* HARTZOG & SOLOVE, *supra* note 502, at 118–19.

514. *See id.* at 48, 49.

515. Scott J. Shackelford, Anne Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, 25 YALE J.L. & TECH. 86, 95 (2023).

516. HARTZOG & SOLOVE, *supra* note 502, at 53.

517. *See* Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 815–16 (2020); HARTZOG & SOLOVE, *supra* note 502, at 51.

518. LabMD v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018).

519. AMG Cap. Mgmt., LLC v. FTC, 593 U.S. 67, 67 (2021).

520. Kosseff, *supra* note 517, at 819.

E. Who Benefits

Welfare fraud detection algorithms feed on power imbalances. Who is benefitting from systems that falsely accuse members of marginalized populations of fraud; that fail to identify legitimate fraud; and that fail to deliver on their contractual obligations?[521] Dan Hatcher has written about how "human service agencies are partnering with private companies to form a vast poverty industry, turning America's most vulnerable populations into a source of revenue."[522] Governments seek to "bolster state coffers," while private companies seek to maximize profits.[523] In this "iron triangle," the vulnerable lose out.[524] In an era of shrinking state budgets and neoliberal commitments to individual responsibility, the state benefits from demonizing needy people as likely fraudsters and from limiting their access to the social safety net through faulty determinations that are difficult to challenge. Interviews with welfare fraud investigators uncovered how "[o]rganizational imperatives encourage investigators to see and substantiate rule violations as deliberate, which is crucial to program retrenchment via fraud control interventions . . . ."[525] By recouping overpayments, states attempt to fill their own coffers.

At the same time, austerity policies preserve a steady surplus of low-wage workers for corporations, who pay low wages that are in turn supplemented by public benefits.[526] Businesses also benefit from the profits earned from selling fraud detection systems to the states, even when they are faulty.[527] In 2021, the welfare automation business was

---

521. This question is inspired by the work of anthropologist Laura Nader, who argued for "studying up," or studying the middle and upper classes, and not only the poor and disadvantaged: "for such institutions and their network systems affect our lives and also affect the lives of people that anthropologists have traditionally studied all around the world." Laura Nader, *Up the Anthropologist: Perspectives Gained from Studying Up*, in REINVENTING ANTHROPOLOGY 9 (Dell Hymes ed. 1974).

522. DANIEL L. HATCHER, THE POVERTY INDUSTRY: THE EXPLOITATION OF AMERICA'S MOST VULNERABLE CITIZENS 1 (Nancy E. Dowd ed., 2016).

523. *Id.* at 2.

524. *See id.* at 53. "The 'iron triangle' is a political science model that describes the self-serving interrelationships between government and the private sector and their influence over government policy and funding." *Id.*

525. Spencer Headworth, *Broke People, Broken Rules: Explaining Welfare Fraud Investigators' Attributions*, 23 PUNISHMENT & SOC. 24, 26 (2020).

526. *See generally* FRANCES FOX PIVEN & RICHARD A. CLOWARD, REGULATING THE POOR: THE FUNCTIONS OF PUBLIC WELFARE (updated ed. 1993) (arguing that restrictions on social assistance programs serve to force poor people into the labor market, and conversely, in times of unrest social assistance is expanded to quell disorder).

527. DONALD COHEN & ALLEN MIKAELIAN, THE PRIVATIZATION OF EVERYTHING: HOW THE PLUNDER OF PUBLIC GOODS TRANSFORMED AMERICA AND HOW WE CAN FIGHT BACK 158 (2021) ("In our society's widening division between the superrich and struggling working families, privatization actively generates schemes that exist primarily to take money from those who have the least and give it to those who have the most.").

estimated to value $440 billion worldwide.[528] Fraud detection is an active piece of this market. In 2021, the Department of Labor entered a contract ultimately worth $528 million with LexisNexis for UI fraud detection, and the Department of Labor also has a separate $2 billion contract involving LexisNexis and TransUnion, a credit monitoring agency.[529] The IRS has a $73 million contract with Accenture for fraud prevention.[530]

During the pandemic, a company called Id.me contracted with numerous states to conduct identity verification for UI programs.[531] A congressional committee later found the company had baselessly overstated the amount of UI fraud in a marketing scheme to get additional contracts.[532] Meanwhile, Id.me's systems did not work as promised, as the system failed to recognize thousands of people who could not reach the back-up call centers.[533] Nevertheless, Id.me has expanded its reach,

528. Morgan Meaker, *The Fraud-Detection Business Has a Dirty Secret*, WIRED (May 7, 2023, at 07:00 ET), https://www.wired.com/story/welfare-fraud-industry/ [https://perma.cc/GS2S-BAKN].

529. Alfred Ng, *Data Brokers Raise Privacy Concerns — But Get Millions from the Federal Government*, POLITICO (Dec. 21, 2022, at 04:30 ET), https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600 [https://perma.cc/6MME-TDF6].

530. *Id.*

531. *See* Rachel Metz, *Want Your Unemployment Benefits? You May Have to Submit to Facial Recognition First*, CNN BUS. (July 23, 2021, at 14:40 ET), https://www.cnn.com/2021/07/23/tech/idme-unemployment-facial-recognition/index.html [https://perma.cc/C3SW-WBH9]; Mia Sato, *The Pandemic Is Testing the Limits of Face Recognition*, MIT TECH. REV. (Sep. 28, 2021), https://www.technologyreview.com/2021/09/28/1036279/pandemic-unemployment-government-face-recognition [https://perma.cc/A2HC-28JQ]; Drew Harwell, *IRS Abandons Facial Recognition Plan After Firestorm of Criticism*, WASH. POST (Feb. 7, 2022), https://www.washingtonpost.com/technology/2022/02/07/irs-idme-face-scans [https://perma.cc/JV2H-5RVC].

532. *See* Alfred Ng, *House Dems Say Facial Recognition Company Made "Baseless Claims*," POLITICO (Nov. 22, 2022, at 17:11 ET), https://www.politico.com/news/2022/11/17/house-dems-say-facial-recognition-company-made-baseless-claims-00069156 [https://perma.cc/2REJ-TFG7].

533. *See* Todd Feathers, *Facial Recognition Failures Are Locking People Out of Unemployment Systems*, VICE (June 18, 2021, at 19:27 ET), https://www.vice.com/en/article/facial-recognition-failures-are-locking-people-out-of-unemployment-systems/ [https://perma.cc/9D5D-BDBY]; *Chairs Maloney, Clyburn Release Evidence Facial Recognition Company Id.me Downplayed Excessive Wait Times for Americans Seeking Unemployment Relief Funds*, House Comm. on Oversight & Gov't Reform (Nov. 17, 2022), https://oversightdemocrats.house.gov/news/press-releases/chairs-maloney-clyburn-release-evidence-facial-recognition-company-idme [https://perma.cc/7F8S-J7T5] (noting that Id.me reported to the committee that ten to fifteen percent of users were unable to verify their identities through the automated system, thus "potentially hundreds of thousands of employment workers were routed to verify their identities through video chats" which had average wait times of more than four hours).

now with more than sixty million users across seventeen federal agencies and forty-two state agencies.[534]

The consulting firm Deloitte is dominant in the automation of public benefits systems, and twenty-five states have awarded it contracts to determine Medicaid eligibility at a worth of $5 billion.[535] Its systems "have generated incorrect notices to Medicaid beneficiaries, sent their paperwork to wrong addresses, and been frozen for hours as a time," and taken "months to fix problems."[536] Deloitte is also active in fraud detection, and during the pandemic it secured contracts worth at least $410 million.[537] However, the systems failed to detect or prevent actual fraud worth an estimated $22.2 billion.[538] After the MiDAS debacle, Michigan hired Deloitte in 2023 to implement a new UI system, and by mid-2025 it was a year overdue and $20 million over budget.[539] This is a form of true fraud — earning taxpayer money to deliver a faulty and harmful product, avoiding accountability, and instead being rewarded with additional contracts. This form of corporate fraud is rarely demonized or stigmatized. It is business as usual.

---

534. *More Than 60 Million Americans Enrolled with ID.me to Safely Verify Their Identity Online*, ID.ME (Aug. 13, 2024), https://network.id.me/press-releases/more-than-60-million-americans-enrolled-with-id-me-to-safely-verify-their-identity-online/ [https://perma.cc/Q6NF-CBL7].

535. Rachana Pradhan & Samantha Liss, *Medicaid for Millions in America Hinges on Deloitte-Run Systems Plagued by Errors*, KFF HEALTH NEWS (June 24, 2024), https://kffhealthnews.org/news/article/medicaid-deloitte-run-eligibility-systems-plagued-by-errors/ [https://perma.cc/67PQ-DQSJ].

536. *Id.*; *see also* In the Matter of Deloitte Consulting LLP, Complaint and Request for Investigation, Injunction and Other Relief to the Federal Trade Comm'n Submitted by National Health Law Program, Electronic Privacy Information Center, and Upturn, Inc. (Jan. 31, 2024), https://healthlaw.org/wp-content/uploads/2024/01/NHeLP-EPIC-Upturn-FTC-Deloitte-Complaint.pdf [https://perma.cc/XTU9-WA6K]; Supplemental Information Concerning In re: Deloitte Consulting LLP (Oct. 16, 2024), https://www.upturn.org/work/supplemental-evidence-to-our-federal-trade-commission-deloitte-complaint/ [https://perma.cc/XTU9-WA6K] (both documents requesting the FTC to investigate Deloitte for its faulty, automated Medicaid eligibility system in Texas and describing errors resulting in lost Medicaid coverage in multiple other states).

537. *See* Thomas Brewster, *States Spent Millions on Deloitte's "Anti-Fraud" Covid Unemployment Systems. They Suffered Billions in Fraud*., FORBES (Nov. 3, 2022, at 08:05 ET), https://www.forbes.com/sites/thomasbrewster/2022/10/31/covid-pandemic-fraud-hits-billions-despite-deloitte-contracts-worth-hundreds-of-millions/ [https://perma.cc/T9MF-4KF2].

538. *See id.*

539. *See* Victor Skinner, *Gretchen Whitmer's Unemployment Website Overhaul Is 14 Months Behind Schedule, $20 Million Over Budget*, MIDWESTERNER (June 11, 2025), https://www.themidwesterner.news/2025/06/gretchen-whitmers-unemployment-website-overhaul-is-14-months-behind-schedule-20-million-over-budget/ [https://perma.cc/NB7N-LESV]. Deloitte blamed issues "on both sides." *Id.*

VI. STRATEGIES FOR FLIPPING THE FRAUD-FIRST PRESUMPTION

The fraud-first presumption underlying fraud detection algorithms is lining the pockets of corporations, but it is not serving the needy or preventing criminals from stealing benefits. Significantly, "[t]his fraud-centric design comes at the expense of the most marginalized members of the workforce — workers of color, low-income workers, and women."[540] It undermines the government's core purpose to serve its citizens and strips people of their dignity.

As the prior discussion demonstrates, evidence of the fraud-first presumption is abundant. Notably, government assistance programs that serve wealthier Americans, such as Medicare, do not embed the same levels of surveillance.[541] Moreover, government agencies are far more concerned with overpayments than with underpayments (the failure to deliver full benefits to eligible claimants).[542] One former social services caseworker explained the realities on the ground:

> Eligibility workers are often better trained to look for fraud than they are to provide trauma-informed care or to refer families to other assistance to address the many challenges of living in poverty. Perversely, case workers can be penalized or jeopardize their jobs for accidentally approving recipients for more benefits than they are eligible for but face no repercussions for denying people benefits that they are eligible for.[543]

---

540. Monée Fields-White, Vivian Graubard, Alberto Rodriguez, Nikki Zeichner & Cassandra Robertson, *Unpacking Inequities in Unemployment Insurance, Public Interest Technology New Practice Lab*, NEW AM. 15 (Sep. 17, 2020), https://www.newamerica.org/pit/reports/unpacking-inequities-unemployment-insurance/a-focus-on-fraud-over-accessibility-the-punitive-design-of-ui/ [https://perma.cc/KBV4-SJH8].

541. *See supra* note 154, at 18 ("Although Medicare . . . also covers various short-term homecare services, a corresponding mandate to use EVV systems has not been imposed on beneficiaries of this government program. Similarly, families that can afford to pay for services out-of-pocket are not subjected to these forms of scrutiny.").

542. *See* Fields-White et al., *supra* note 540, at 17 ("By focusing on overpayments, the department [of labor] is not held accountable for determining other errors created by the state, or even an employer, when it comes to UI payments — such as underpayments — which are also payment inaccuracies.").

543. Parker Gilkesson, *A Caseworker's View: "Intentional Program Violations" Cause More Harm Than Good*, CTR. FOR L. & SOC. POL'Y (Mar. 3, 2022), https://www.clasp.org/blog/caseworker-s-view-intentional-program-violations-cause-more-harm-good/ [https://perma.cc/H29N-Y4EH].

Other system actors such as caseworkers or employers who obtain benefits for which they are ineligible get far less scrutiny or punishment than claimants.[544]

Meanwhile, agencies serving low-income people have placed the burden of disproving fraud on recipients, rather than the social service agencies. A Colorado study of food stamp fraud hearings found that administrative law judges accepted minimal evidence to find clear and convincing evidence of fraudulent intent, such as a claimant's signature on a complex sixteen-page application with highly technical questions.[545] The authors concluded that decisions "seemingly rely on presumption of intent, rather than requiring the counties to identify elements of the required standard of proof and introduce sufficient evidence to prove each element."[546] Such presumptions undermine the burden of proof. Algorithms are programmed to equate innocent errors with fraud[547] — and even some state agencies define fraud to include mistakes. In this "anything goes" atmosphere, vendors are using sloppy coding, knowing they face no consequences. On the contrary, they are often rewarded with lucrative contracts even after their misdeeds come to light.

To move to a support-first presumption that recognizes the dignity of claimants, we need to rethink governance over fraud by restraining the impact of surveillance capitalism on welfare fraud detection algorithms and adding safeguards to the datafied state. There are many sound recommendations in the algorithmic accountability literature that would help improve the fairness, accountability, and transparency of welfare fraud detection algorithms.[548] This Part focuses specifically on mechanisms for flipping the fraud-first presumption to a support-first presumption.

---

544. One legal services attorney handling UI cases during the MiDAS debacle commented: "If you believe that the automated system is good for detecting fraud, then it should be good at detecting fraud against the employers equally with the employees . . . . And it is not being used in that way. And in the cases we've done, we've seen employer fraud every bit as much as we've seen individual fraud committed." Ryan Felton, *Criminalizing the Unemployed*, DETROIT METRO TIMES (July 1, 2015), https://www.metrotimes.com/news/criminalizing-the-unemployed-2353533 [https://perma.cc/F543-J4RB].

545. COLO. CTR. ON L. & POL'Y, *supra* note 412, at 30.

546. *Id.* at 30–31.

547. *See* EPIC Complaint, *supra* note 122, at 13 ("Within its contract with IWD, Pondera characterized the mere presence of improper payments as fraud, even without other indicators of fraud.").

548. For example, the Center on Budget and Policy Priorities recommends that instead of the relentless focus on program integrity, agencies should focus on compassionate integrity, asking: "What share of eligible people participate? Do eligible people receive the benefits for which they qualify? How accurate are eligibility and benefit determinations? How smooth is the appeals process?" Alicia Huguelet, Dottie Rosenbaum & Jennifer Wagner, *What We Measure Matters: Enhanced Performance Metrics for SNAP and Medicaid Would Promote a More Human-Centered Delivery System*, CTR. ON BUDGET & POL'Y PRIORITIES 4 (Aug. 30, 2023), https://www.cbpp.org/sites/default/files/8-30-23fa.pdf [https://perma.cc/XV9Y-2NUX].

(1) Eliminate Fraud Terminology

To begin with, we must codify as a matter of law and computer programming that unintentional errors and mistakes involving claimants in social service systems are not fraud. Administrative cases involving "possible overpayments" should avoid fraud terminology altogether, or at least not until a human adjudicator has determined by a preponderance of the evidence that the claimant has acted with the requisite intent. Fraud is a loaded and stigmatized term with criminalized implications.[549] It constitutes a small percentage of cases. It does not apply to most needy people who turn to the government for support. The repeated, rhetorical linkage between "fraud" and governmental assistance discourages people from seeking needed support and reduces public support for the social safety net. The term should be jettisoned.

(2) Reduce Administrative Burdens

Although fraud rates are low, overpayments and underpayments are a routine outcome of public benefits systems. States should thus focus on lowering rates of inaccurate payments. The goal should not be tamping out every incident of fraud and spending massive resources to do so, but ensuring programs meet the needs of eligible people.[550] Claimants currently face numerous "administrative burdens" in the application process that can not only lead to wrongful accusations of fraud, but also discourage people from seeking state support (which may be the purpose).[551] These burdens include "significant pain points in eligibility and application processes for knowing where to start, sourcing documents to prove eligibility, and online access."[552]

---

549. SNAP and some TANF programs use the term "intentional program violations" as a synonym for fraud, but this too is problematic because it assumes wrongful intent. *See, e.g.*, 7 C.F.R. § 273.16.

550. As Professors Herd and Moynihan wrote,

> The question 'are we going to tolerate any fraud?' is very different from the question of 'how much fraud are we willing to tolerate given impacts on access?' The latter question implies a willingness to consider tradeoffs, which in turn requires evidence. Private companies, such as credit card companies or grocery stores, make these tradeoffs all the time, accepting some measure of theft or fraud rather than imposing a set of requirements that make services impossible to access.

Pamela Herd & Donald Moynihan, *Administrative Burdens in the Social Safety Net*, 39 J. ECON. PERSPS. 129, 138 (2025).

551. *See* PAMELA HERD & DONALD P. MOYNIHAN, ADMINISTRATIVE BURDEN: POLICYMAKING BY OTHER MEANS 2 (2018) (defining administrative burden as "the costs people encounter when they search for information about public services (learning costs), comply with rules and requirements (compliance costs), and experience the stresses, loss of autonomy, or stigma that come from such encounters (psychological costs).").

552. Ariel Kennan & Sara Soka, *Benefit Eligibility Rules as Code: Reducing the Gap Between Policy and Service Delivery for the Safety Net*, BEECK CTR. FOR SOC. IMPACT & INNOVATION 8 (Feb. 2022), https://digitalgovernmenthub.org/wp-content/uploads/2022/07/Benefit-Eligibility-Rules.pdf [https://perma.cc/LCF8-ZGYQ].

Simplifying public benefits eligibility standards can reduce confusion and mistakes committed by claimants and caseworkers. In addition, agencies can streamline application and verification processes by using plain English in explaining program requirements, harmonizing requirements across programs, and using human-centered design in their technology.[553] Studies have shown that simplifying public benefits processes does not increase fraud, while helping people obtain needed benefits.[554] Further, these practices reinforce the dignity and humanity of claimants.[555]

(3) Adopt Rules as Code Approach

To improve accuracy, policy experts also recommend a "rules as code" approach, which involves drafting statutes and regulations in a "machine-consumable form, which allows rules to be understood and actioned by computer systems in a consistent way."[556] This would counter known problems that programmers are creating when they inaccurately translate legal rules into computer code, which in turn creates mistakes that result in fraud allegations.[557] Indeed, an audit of a state eligibility screening tool for five different safety net programs found major coding errors in violation of statutory requirements, leading the authors to conclude "there is a vast difference between what the law says, and what the tool does."[558] Adopting "rules as code" would also improve the explainability of algorithmic outcomes, thus aiding claimants to better understand and challenge agency decisions.[559] In

553. *Id.* at 12–13; Heather Hahn, Eleanor Pratt & Sarah Knowles, *Strategies for Improving Public Benefits Access and Retention*, URB. INST. 6–8 (Jan. 2023), https://www.urban.org/sites/default/files/2023-01/Strategies%20for%20Improving%20Public%20Benefits%20Access%20and%20Retention.pdf [https://perma.cc/45HE-EHXX]; ASPEN INST., OFF. OF MGMT. & BUDGET OF HEALTH & HUM. SERVS. & U.S. DEPT. OF AG., IMPROVING ACCESS TO PUBLIC BENEFITS AND CUSTOMER EXPERIENCE (2022), https://assets.performance.gov/cx/files/life-experiences/2024/ffs/FFS_Best_Practices.pdf [https://perma.cc/W7F5-5UM2].

554. Sabinne Lee, *Impact of Administrative Burden on Inappropriate Payment Error: A Blessing or a Curse?*, 26 INT'L. REV. PUB. ADMIN. 18 (2020).

555. Hahn et al., *supra* note 553, at 7–8 (describing a range of practices to respect the dignity and humanity of clients).

556. Kennan & Soka, *supra* note 552, at 14 (quoting James Mohun & Alex Roberts, *Cracking the Code: Rulemaking for Humans and Machines*, 42 OECD WORKING PAPERS ON PUB. GOVERNANCE 1, 2 (Oct. 2020), https://www.oecd.org/innovation/cracking-the-code-3afe6ba5-en.html [https://perma.cc/2QAU-SSFE]).

557. *See* Nel Escher & Nikola Banovic, *Exposing Error in Poverty Management Technology: A Method for Auditing Government Benefits Screening Tools*, 4 PROC. ACM HUM.-COMPUT. INTERACT. 1, 17 (May 2020), https://doi.org/10.1145/3392874 [https://perma.cc/K4WA-MUVN].

558. *Id.* at 17. The authors recommend that "[t]o decide the appropriate balance between correctness and convenience, software engineers and legal experts should work together. Software engineers write the tool logic that determines how ambiguity is resolved, but legal experts might have a better understanding of how the trade-offs will affect the applicant populations." *Id.* at 16.

559. *See* Huq, *supra* note 345, at 1946–47 (describing different modes of explanation).

addition, it would assist decision-makers in rendering sound decisions and regulators in overseeing algorithmic tools.[560] If an algorithmic system is too complicated to explain outcomes, then that tool should not be used in the social services context.

(4) Require Pre-Testing of Algorithms

To further improve accuracy, agencies should subject fraud detection algorithms to rigorous pre-testing before they are deployed. Many proposals to enhance algorithmic accountability recommend algorithmic impact assessments ("AIAs") and audits, and some jurisdictions in the United States and abroad have enacted variations of these requirements. In general, AIAs involve assessing the risks of algorithmic tools to mitigate harms before deployment.[561] Audits involve "inspecting the working of a particular algorithmic system, in order to understand its functioning, and assess it with respect to some predefined normative standard."[562] AIAs are generally carried out prior to deployment, whereas audits are conducted throughout an algorithm's lifespan to ensure a system is operating as expected.[563] Both approaches would improve welfare fraud detection algorithms by identifying potential risks and tracking them over time.

However, given the well-documented rates of false positives and false negatives in fraud detection algorithms, pre-deployment testing also needs to be a legally required feature mandate for these systems. Claimants should not be guinea pigs in a system-wide algorithmic rollout. Indeed, the technical literature acknowledges the difficulties of designing fraud detection algorithms given the low rates of fraud on

560. *See* Oluwabusayo Adijat Bello, Adebola Folorunso, Jane Onwuchekwa & Oluomachi Eunice Ejiofor, *A Comprehensive Framework for Strengthening USA Financial Cybersecurity: Integrating Machine Learning and AI in Fraud Detection Systems*, 11 EURO. J. COMP. SCI. & INFO. TECH. 62, 73 (2023) ("Transparent and interpretable models enable analysts to understand how predictions are generated, identify potential biases or errors, and make informed decisions based on model outputs.") (citation omitted); Brauneis & Goodman, *supra* note 458, at 127 ("When algorithmic output is uninterpretable — when the decision path is not explained — government officials have no way of knowing whether and how the factors they are facing accord with the factors that produced the algorithmic recommendation.").

561. ADA LOVELACE INST., AI NOW INST. & OPEN GOV. PARTNERSHIP, ALGORITHMIC ACCOUNTABILITY FOR THE PUBLIC SECTOR: LEARNING FROM THE FIRST WAVE OF POLICY IMPLEMENTATION 21 (2021). AIAs are modelled after impact assessments frameworks in other regulatory areas, such as environmental and privacy law. *See id.* at 24. *See generally* Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J.L. & TECH. 117 (2021).

562. ADA LOVELACE INST., *supra* note 561, at 24. They are often carried out by external actors. *Id.*; *see also* Miranda Bogen, *Assessing AI: Surveying the Spectrum of Approaches of Understanding and Auditing AI Systems*, CTR. FOR DEM. & TECH. 48 (Jan. 2025).

563. *See* ADA LOVELACE INST., *supra* note 561, at 24; Mona Sloane & Emanuel Moss, *Assessing the Assessment: Comparing Algorithmic Impact Assessments and AI Audits* (June 20, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4486259 [https://perma.cc/9264-MQZ3] (comparing the ex ante and ex post purposes of each tool).

which to train algorithmic models.[564] Due to the lack of available training data, an "anomalous transaction does not necessarily mean a problematic transaction."[565] Further, in deploying algorithms, there can be a conflict between efficiency and accuracy. "[R]educing administrative errors helps to overcome this conflict — *but only when the objective function is to identify and minimize all error types, not just politically salient ones*."[566] In other words, identifying underpayments is as important as reducing overpayments, the latter of which also requires separating innocent errors from intentional misconduct and not painting them together with a broad brush. Thus, testing for correctness and setting accuracy benchmarks are essential on the front end.

(5) Data Reporting

On the back end, technology vendors and state agencies should publicly report data related to their fraud detection systems. This reporting should include rates of accusations, the basis of the accusations, measures taken to inform claimants of accusations, the rates of appeals in which claimants appear, the number of claims that are adjudicated as intentional fraud as well as those result from honest mistakes, rates of identity theft and cybercrime, and the rates of false positive and false negative accusations. Machine learning models should be evaluated not only for their accuracy, but also audited for their safety, reliability, and equity.[567] All these evaluations should be publicly reported. Where initial accusations are ultimately found to lack merit, vendors should be

564. "It is hard for algorithms to learn when samples are really unbalanced as they do not frequently encounter fraud cases. The existing literature is aware of this problem and has resorted to various methods to deal with this challenge." Yang Bao, Hilary Gilles & Bin Ke, Artificial Intelligence and Fraud Detection in INNOVATIVE TECHNOLOGY AT THE INTERFACE OF FINANCE AND OPERATIONS 226 (Volodymyr Babich, John R. Birge & Gilles Hilary eds. 2022); *see also* Yisong Chen, Chuqing Zhao, Yixin Xu, Chuanhao Nie & Yixin Zhang, *Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications*, DATA SCI. & MGMT. 5 (Aug. 2025), https://doi.org/10.1016/j.dsm.2025.08.002 [https://perma.cc/5WGJ-DUKM] (discussing that the challenge to algorithmic fraud detection is its rarity, which "leads to highly imbalanced datasets that impair model training and evaluation").

565. Bao et al., *supra* note 564, at 235.

566. Matthew M. Young, Johannes Himmelreich, Danylo Honcharov & Sucheta Soundarajan, *Using Artificial Intelligence to Identify Administrative Errors in Unemployment Insurance*, 39 GOV. INFO. Q. 1, 2 (Oct. 2022).

567. *See generally* Edwin A. Farley & Christian R. Lansang, *AI Auditing: First Steps Towards the Effective Regulation of Artificial Intelligence Systems*, 38 HARV. J.L. & TECH. 1 (2025) (proposing audit standards for AI data, models, and deployment); NAT'L INST. OF STANDARDS & TECH, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK 1.0 28–31 (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [https://perma.cc/LNV2-3RGS] (proposing a framework for responsible management of AI risks, including measurement processes); Ellen P. Goodman & Julia Trehu, *Algorithmic Auditing: Chasing AI Accountability*, 39 SANTA CLARA HIGH TECH. L.J. 289 (2023) (discussing ways to make algorithmic audits reliable accountability mechanisms); Shea Brown, Jovana Davidovic & Ali Hasan, *The Algorithm Audit: Scoring the Algorithms that Score Us*, BIG DATA & SOC. 1 (2021) (providing a framework for an ethical audit).

required to pay a penalty to the state. This would ideally push vendors to increase the accuracy of their fraud detection systems. In addition, to identify possible bias in an automated system, it is important to report on the race, ethnicity, gender, age, disability status, and geography of claimants accused of fraud, and to track the accuracy of fraud determinations by these groups through the appeals process.

(6) Adopt Substantive Requirements for Fraud Detection Algorithms

Post hoc litigation after people suffer serious injuries is not an adequate remedy for the false positives that plague welfare fraud detection algorithms, and it has not led to systemic design improvements. Simply put, individualized due process hearings are vitally important, but do not fix structural flaws around accuracy and bias in fraud detection algorithms. Claimants need more than notice and hearings. Welfare fraud detection algorithms should be governed by substantive, codified standards of accuracy, non-discrimination, accountability, transparency, data privacy, and cybersecurity.[568] Claimants should have individual legal rights to enforce these standards, but agency regulation and oversight is also essential.[569] These standards should also be set forth in procurement contracts.[570] Agencies should contract for the ability to cancel poorly performing algorithmic systems pursuant to strict and clear benchmarks and without penalty.[571] Establishing these substantive standards should involve input from impacted people, community organizations, civil society groups, and advocates.[572]

(7) Bring Public Participation into AI Governance

There is a rich literature about bringing public participation into AI governance, given the ways that meaningful input can add on-the-ground expertise and improve decision-making, while enhancing trust between the state and its citizens.[573] Impacted people can be

568. *See* Huq, *supra* note 345, at 1941 (arguing for substantive regulatory interventions that are ex ante).

569. Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 978–79 (2023) ("The ability of individuals to exercise control over their personal data is quite limited; there is a ceiling to individual control.").

570. *See* Mulligan & Bamberger, *supra* note 488, at 781–82 (explaining that procurement should be viewed as a policymaking process).

571. *See* Brauneis & Goodman, *supra* note 458, at 164–66 (noting that procurement can be a form of algorithmic governance).

572. Bogen, *supra* note 562, at 63 ("AI systems are not just technical artifacts, but sociotechnical systems where people, institutions, and technologies interact; understanding the impacts of these systems therefore requires interdisciplinary and mixed-method approaches.").

573. *See, e.g.*, Christine Galvagna, *Inclusive AI Governance: Civil Society Participation in Standards Development*, ADA LOVELACE INST. (Mar. 2023),

particularly insightful in helping with platform design, playing a role in pre-testing, and identifying appropriate algorithmic triggers (such as irregular patterns and anomalies) for possible overpayments. It seems that current fraud detection algorithms are relying on predictive factors that misunderstand the lives of low-income people.[574] For instance, in some jurisdictions, UI fraud triggers include receipt of too many applications from a single household, despite the facts that certain ethnic groups often live in multi-generational households and some low-income people use homeless shelters as their official addresses.[575] Deeper involvement by impacted people and service providers would identify more accurate triggers for possible over- and under- payments, as well as improve system design overall.[576]

Given the unrestrained data flows of surveillance capitalism, designers of welfare fraud detection algorithms need to identify more accurate triggers for identifying nefarious actors who are preying upon the technological weaknesses of these systems. A range of stakeholders should be weighing in on algorithmic design choices, such as acceptable rates of false positives and false negatives, as these are policy choices, and not purely technical ones. Values of fairness, efficiency, and accuracy need to be surfaced and debated through democratic means.[577] Similarly, states, the federal government, and contractors need to cross-collaborate on effective technologies in fraud detection, as the "problem concerns the whole of government and whole of society."[578] Governments need to adequately fund technological systems and the human staff to oversee them.[579] In addition, other industries

---

https://www.adalovelaceinstitute.org/report/inclusive-ai-governance/ [https://perma.cc/L2GT-RENS]; Michele E. Gilman, *Beyond Window Dressing: Public Participation for Marginalized Communities in the Datafied Society*, 91 FORDHAM L. REV. 503 (2022); Ngozi Okidegbe, *To Democratize Algorithms*, 69 UCLA L. REV. 1688 (2023); Margo Kaminski, *Voices In, Voices Out: Impacted Stakeholders and the Governance of AI*, 71 UCLA L. REV. 176 (2024).

574. *See* NATL. ACAD. OF SOC. INS., UNEMPLOYMENT INSURANCE TASK FORCE: FINAL REPORT 11 (2024), https://www.nasi.org/wp-content/uploads/2024/07/Unemployment-Insurance-Task-Force-Final-Report.pdf [https://perma.cc/U9FF-8URT] ("Currently, states are employing multiple interventions to detect and prevent fraud, but little data is available about which interventions are the most effective and which are more likely to waste agency staff time and hold up innocent claimants who need benefits.").

575. Fields-White et al., *supra* note 540, at 17.

576. *See* Bao et al., *supra* note 564, at 231 ("One may be tempted to throw in as many predictors as possible into a machine learning model for training and prediction, but . . . more predictors do not necessarily improve prediction performance.").

577. *See* Unai Fischer-Abaigar, Christoph Kern, Noam Barda & Frauke Kreuter, *Bridging the Gap: Towards an Expanded Toolkit for AI-Driven Decision-Making in the Public Sector*, 41 GOVT. INFO. Q. 1, 5 (2024) (urging stakeholder input into competing objectives).

578. NAT'L ACAD. OF SOC. INS., *supra* note 574, at 2.

579. *See* Michele Evermore & Laura Valle Guitierrez, *The Pandemic and Unemployment Insurance Fraud*, CENTURY FOUND. (Feb. 8, 2023), https://tcf.org/content/commentary/the-pandemic-and-unemployment-insurance-fraud/ [https://perma.cc/K6FQ-TVAZ] ("[W]e need

with a greater motive to accurately identify fraud include banking, insurance, and health care, and they can offer lessons for social services.

(8) Keep Humans in the Loop

These debacles outlined in the case studies demonstrate the need to keep humans in the loop[580] — but these humans need to be knowledgeable and themselves subject to oversight.[581] In the datafied state, public engagement has moved from street-level bureaucrats to screen-level and even system-level bureaucracies, in which it is increasingly harder for citizens to communicate with diminishing numbers of agency staff.[582] Yet "[m]achine decision-making currently cannot incorporate emotion, morality, or value judgments, which are essential components of decisions involving people's welfare."[583] In the case studies, computerized systems made determinations of fault without staff input and without meaningful opportunities for the accused to understand the basis of the decision or to contest it. Keeping humans in the loop can help

---

to do more to recognize the cost of technology. Right now, states do not have the right funding to be able to set aside what is needed for the kinds of continual technological improvements that really should be made every year.").

580. "Human in the loop" is defined as "an individual involved in a single, particular algorithmic decision." Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 VAND. L. REV. 429, 434 (2023). "[I]f a human has the ability to intervene in an individual decision — to change it, approve it, or immediately implement it — then there is a human 'in' the loop." *Id.* at 441. The GDPR, governing data privacy in the European Union, requires a human in the loop for decisions with legal or significant effects, providing that "[t]he data subject shall have the right not to be subject to a decision based solely on fully automated data processing." Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 22(1), 2016 O.J. (L 119) (EU).

581. For example, the fraud scandal in Minnesota, in which criminal syndicates created fake entities and/or lied about clients served to steal money across numerous public benefits programs, has been tied to agency officials' failure to investigate complaints and irregularities due to fear of litigation and alienating the politically powerful Somali community, where some, but not all, of the fraud originated. *See* Ernesto Londono, *How Fraud Swamped Minnesota's Social Services System on Tim Walz's Watch*, N.Y. TIMES (Jan. 7, 2026), https://www.nytimes.com/2025/11/29/us/fraud-minnesota-somali.html [https://perma.cc/RGK8-A7E4]; OFF. LEGIS. AUDITOR, STATE OF MINN., MINNESOTA DEPARTMENT OF EDUCATION: OVERSIGHT OF FEEDING OUR FUTURE; SPECIAL REVIEW 3–4 (2024), https://www.auditor.leg.state.mn.us/sreview/pdf/2024-mdefof.pdf [https://perma.cc/XNQ4-WWLS]. Prosecutions of these cases began under the Biden Administration and continue under the second Trump Administration. *See* Londono, *supra* note 581. Minnesota Governor Walz's fraud prevention program will use AI to identify fraud. *See* Colin Wood, *Minnesota's Expanded Anti-Fraud Efforts Include AI Pilot Project*, STATESCOOP (Jan. 7, 2025), https://statescoop.com/minnesota-fraud-tim-walz-anti-fraud-expansion-ai/ [https://perma.cc/MX4W-3W5V].

582. Mark Bovens & Stavros Zouridis, *From Street-Level to System-Level Bureaucracies: How Information and Communication Technology Is Transforming Administrative Discretion and Constitutional Control*, 62 PUB. ADMIN. REV. 174, 175 (2002).

583. Daniel J. Solove & Hideyuki Matsumi, *AI, Algorithms, and Awful Humans*, 92 FORDHAM L. REV. 1923, 1925 (2024).

avoid these problems, but only if the humans exercise their discretion and oversight wisely.

Decisions regarding a "possible overpayment" should be rendered by a human, even if initially flagged by an algorithmic system. Agencies must improve their technological expertise to oversee welfare fraud detection algorithms and to train decision-makers about the fallibility of algorithmic determinations.[584] Impacted claimants should have opportunities to communicate with staff, as studies show that the acceptability of algorithmic decisions "in the public's eyes hinges on effective human communication during the decision-making process."[585] Keeping humans in the loop at various stages of the fraud determination process serves the goals of providing individualized reasons for determinations, keeping agencies accountable to the people they serve, and respecting the dignity of claimants, who should not be reduced to abstract data points when their well-being hangs in the balance.[586]

Many situations of possible overpayments involve the question: Was it an innocent mistake or was it an intentional attempt to wrongfully obtain benefits? While well-designed algorithms can identify whether someone meets an eligibility standard, algorithms do not yet accurately or fairly read people's minds. Agencies will thus not only need to retain and train staff that can understand and oversee their algorithmic systems but also staff to interface with claimants and to investigate possible over and under payments. Agency staff will need to be trained in, and screened for, the ways that they can be biased when engaging with automated decision-making, such as automation bias (the psychological tendency to believe algorithmic outputs due to their perceived objectivity) and selective adherence (the propensity to follow algorithmic outputs that coincide with pre-existing beliefs).[587]

* * * * *

584. *See* U.S. GOV'T ACCOUNTABILITY OFF., FRAUD AND IMPROPER PAYMENTS: DATA QUALITY AND A SKILLED WORKFORCE ARE ESSENTIAL FOR UNLOCKING THE BENEFITS OF ARTIFICIAL INTELLIGENCE 10 (Apr. 9, 2025), https://www.gao.gov/assets/880/876842.pdf [https://perma.cc/X2BP-3N47] (describing a "severe shortage of federal staff with AI expertise" and identifying "mission-critical gaps in federal workforce skills").

585. Haim & Yogev, *supra* note 421, at 33 (emphasis omitted); *see also* Yoan Hermstrüwer & Pascal Langenbach, *Fair Governance with Humans and Machines*, 29(4) PSYCH., PUB. POL'Y & L. 525, 546 (2023) ("[W]e find for several application contexts that procedures are perceived as fairest when an algorithmic decision aid is accompanied by high human involvement in the decision-making procedure.").

586. *See* Crootof et al., *supra* note 580, at 479, 482, 480. The goal is to combine the best aspects of human and machine decision-making, but this takes careful planning and attention to respective roles; it is by no means assured. *Id.* at 467–73.

587. *See* Saar Alon-Barket & Madalina Busuioc, *Public Administration Meets Artificial Intelligence: Towards a Meaningful Behavioral Research Agenda on Algorithmic Decision-Making in Government*, 7 J. BEHAV. PUB. ADMIN. 1, 4–5 (2024).

In sum, there are a variety of mechanisms for reorienting the datafied welfare state toward supporting people in need and enhancing their dignity by improving the accountability, transparency, and fairness of fraud detection algorithms.

VII. CONCLUSION

Under the second Trump Administration, DOGE wreaked havoc across the federal government by slashing programs, eliminating agencies, firing workers, and depriving citizens of government services.[588] President Trump claimed these actions were necessary to eliminate "billions and billions of dollars in waste, fraud and abuse," which is "one of the reasons [he] got elected."[589] The safety net is in the crosshairs, and AI is being used to scour citizens' personal data and identify fraud. Elon Musk, the tech billionaire and richest person in the world who led DOGE at its inception (before a falling out with the President), targeted entitlement programs as rife with fraud and thus, "the big one to eliminate."[590]

At the SSA, DOGE leaned on the fraud mantra to access sensitive personal data in the agency's database, threatening the security and accuracy of that data and raising the specter that it could be used for surveillance or retribution.[591] President Trump told Congress that millions of non-existent people over the age of 100 were receiving benefits. However, this number was based on a misinterpretation, easily explained, of how the SSA properly handles birth and death dates in its antiquated database.[592] Nevertheless, DOGE — staffed by people with no experience in managing complex government entitlement programs — persisted in advancing this falsehood. DOGE also claimed

---

588. *See* Emily Badger, David A. Fahrenthold, Alicia Parlapiano & Margot Sanger-Katz, *How Did DOGE Disrupt So Much While Saving So Little?*, N.Y. TIMES (Dec. 21, 2025), https://www.nytimes.com/2025/12/23/us/politics/doge-musk-trump-analysis.html [https://perma.cc/F35E-RXSV]; Hannah Natanson & Meryl Kornfield, *The Year Trump Broke the Federal Government*, WASH. POST (Dec. 23, 2025), https://www.washingtonpost.com/politics/interactive/2025/trump-federal-government-workers-doge/ [https://perma.cc/KH2K-WBXR].

589. *See* Hannah Natanson, *DOGE Vowed to Make Government More 'Efficient' — But It's Doing the Opposite*, WASH. POST (June 2, 2025), https://www.washingtonpost.com/business/2025/06/02/doge-vowed-make-government-more-efficient-its-doing-opposite/ [https://perma.cc/JSC6-PAVT].

590. *See* Tess Wilkinson-Ryan, *How the Social Safety Net Became for 'Suckers,'* TIME MAG. (Mar. 18, 2025, at 09:45 ET), https://time.com/7268929/social-security-trump-elon-doge-cuts-suckers-essay/ [https://perma.cc/TQM4-PHYW].

591. *See* Elaine Kamarck, *DOGE is Disrupting Social Security*, BROOKINGS (Mar. 26, 2025), https://www.brookings.edu/articles/doge-is-disrupting-social-security/ [https://perma.cc/28V3-ZQR2].

592. *See* David Gilbert, *No, 150-Year-Olds Aren't Collecting Social Security Benefits*, WIRED (Feb. 17, 2025, at 15:02 ET), https://www.wired.com/story/elon-musk-doge-social-security-150-year-old-benefits/ [https://perma.cc/FE4E-MMFP].

that forty percent of claims made by phone were fraudulent.[593] Yet when the SSA began using AI to conduct anti-fraud checks for phone-based claims and thereby created delays in processing, the agency found that only two out of 110,000 claims had a high probability of being fraudulent.[594]

DOGE made similar, unfounded claims about fraud across the safety net[595] even though its definition of "fraud" remains unclear, and its statistics are routinely debunked.[596] In the name of fraud, governmental assistance is being cut, and millions of people will suffer deprivations of their health, well-being, and financial security, as well as the misuse of their personal data. AI is the tool to effectuate this narrative. The Administration has used the specter of fraud to justify cutting social services funds, primarily to blue states in an act of apparent retribution, which a federal judge temporarily enjoined.[597] The Administration's concern about welfare fraud appears insincere given that President Trump has commuted the sentences of at least sixty-eight people convicted of Medicaid and Medicare fraud, including thirteen

---

593. *See* Alexandra Berzon, Nicholas Nehamas & Tara Siegel Bernard, *The Bureaucrat and the Billionaire: Inside DOGE's Chaotic Takeover of Social Security*, N.Y. TIMES (June 16, 2025), https://www.nytimes.com/2025/06/16/us/politics/doge-social-security.html [https://perma.cc/6YCR-XBAT].

594. *See* Natalie Alms, *SSA Changes Phone Fraud Policies After Finding Very Little Fraud*, NEXTGOV/FCW (May 16, 2025), https://www.nextgov.com/digital-government/2025/05/ssa-changes-phone-fraud-policies-after-finding-very-little-fraud/405380/ [https://perma.cc/5YSK-3AFT]. The agency subsequently ceased the three-day delay in processing, but continued with fraud checks. *Id.*

595. For instance, with regard to UI, DOGE claimed it had uncovered over $400 million in fraudulent claims without disclosing (or realizing) that this had already been uncovered by federal investigators in the Biden Administration. *See* Matt Sedensky, *DOGE Trumpets Unemployment Fraud that the Government Already Found Years Ago*, AP NEWS (Apr. 15, 2025, at 17:32 ET), https://apnews.com/article/doge-trump-musk-unemployment-aa033544cb4e7167d0f310f0f93bbede [https://perma.cc/NTH2-746B]. Similarly, DOGE persists in claiming that fraud prevention requires it to access HHS data systems that manage Medicaid and Medicare. *See* Maya Goldman, *Musk's Team Accesses Medicare, Medicaid Record*s, AXIOS (Feb. 6, 2025), https://www.axios.com/2025/02/06/elon-musk-doge-health-data-cms [https://perma.cc/GC9C-BFJH]. HHS is sharing the data with ICE for immigration enforcement purposes. Kimberly Kindy & Amanda Seitz, *Trump Administration Hands Over Medicaid Recipients Personal Data Including Addresses to ICE*, NBC NEWS (July 17, 2025, at 14:09 ET), https://www.nbcwashington.com/news/politics/trump-administration-hands-over-medicaid-recipients-personal-data-including-addresses-to-ice/3959030/ [https://perma.cc/EN7Z-H9BT].

596. *See* Anne Flaherty & Will Steakin, *DOGE is Searching Through Social Security Payments Looking for Fraud*, ABCNEWS (July 17, 2025, at 14:09 ET), https://abcnews.go.com/Politics/doge-searching-social-security-payments-fraud/story?id=119564143 [https://perma.cc/YVJ5-T9UY]; Natalie Alms, *DOGE Went Looking for Phone Fraud at SSA — and Found Almost None*, NEXTGOV/FCW (May 15, 2025), https://www.nextgov.com/digital-government/2025/05/doge-went-looking-phone-fraud-ssa-and-found-almost-none/405346/ [https://perma.cc/89N9-5DXU].

597. *See* Tony Romm, *In Trump's Fraud Crackdown, Political Foes Face Harshest Scrutiny*, N.Y. TIMES (Feb. 3, 2026), https://www.nytimes.com/2026/02/03/us/politics/trump-fraud-minnesota-snap-medicaid.html?smtyp=cur&smid=bsky-nytimes [https://perma.cc/5M59-H2K3].

wealthy individuals convicted in cases involving more than $1.6 billion in false claims.[598] At the same time, he has defunded internal agency investigators who investigated fraud allegations.[599]

As this article makes clear, DOGE's fraud narrative is provably wrong but potent. It rests on a lengthy history of racialized demonization of the poor as lazy swindlers. The truth, documented in countless government reports, is that most overpayments in public benefit systems result from innocent mistakes by claimants and agencies in trying to comply with extremely complex regulatory regimes, and also from programming errors in technological systems. Still, it is important to acknowledge that criminals are moving into the welfare game, enabled by AI design flaws combined with the unregulated streams of personal data that feed surveillance capitalism. Thus, welfare fraud is not entirely a myth, but it generally is not committed by the people whom it is designed to serve. Law and technology must adapt to this reality.

Unfortunately, current law is inadequate to restrain the ways that AI both generates false fraud accusations and enables real swindlers. In the analog era, a rogue or racist caseworker could wrongfully accuse someone of fraud, but their reach was practically limited, and claimants could contest the allegation in an in-person hearing. By contrast, in the datafied state, an inaccurate or biased algorithm operates at scale, replicating its errors across a vast swath of the claimant population. Indeed, fraud detection algorithms impacting millions of people across the globe have been grossly inaccurate due to faulty programming and predictive analytics based on biased data. Yet fraud detection algorithms are black boxes, lacking transparency, and thus claimants often do not know the basis of the accusation against them — even when the state places the burden on them to prove their innocence. For their part, government officials often do not understand the algorithms they procure, thus undermining the accountability that is foundational to democracy. Meanwhile, fraud detection vendors continue to gross billions of taxpayer dollars while insulating themselves from liability.

In several high-profile algorithmic catastrophes, jurisdictions deployed systems that automatically charged people with fraud and demanded repayments without a meaningful opportunity to be heard. These robo-adjudications undermine any notion of due process. While claimants have successfully pursued lawsuits against these systems, they received compensation years, even decades, after suffering serious emotional, psychological, and financial injuries. And some are still waiting. Ex post solutions are not enough. We must flip the fraud-first

598. *Id.*; Brett Kelman, *Trump's Health Fraud Focus at Odds with Past Pardons*, KFF HEALTH NEWS (Apr. 4, 2025), https://kffhealthnews.org/news/article/the-week-in-brief-trump-health-fraud-pardons/ [https://perma.cc/LJ9Z-2VWM].

599. Romm, *supra* note 597.

presumption codified into AI fraud detection systems in favor of a support-first approach that serves society's most vulnerable people.

The real fraud in the welfare system is not committed by the poor — it is the myth that they do, and the false promise that AI will root it out.