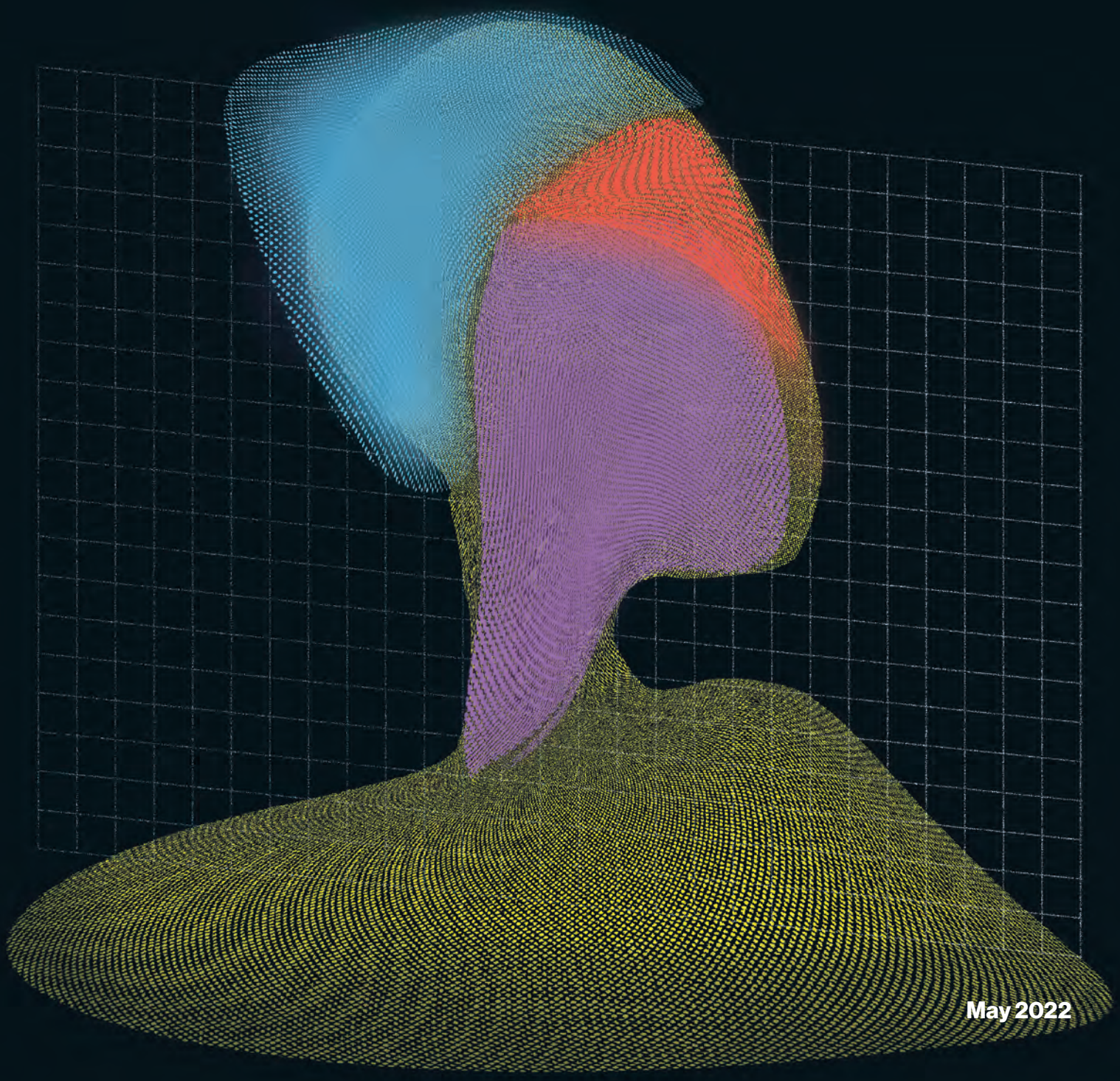
Ableism And Disability Discrimination in New Surveillance Technologies

How new surveillance technologies in education, policing, health care, and the workplace disproportionately harm disabled people



May 2022

The **Center for Democracy & Technology** (CDT) is a 25-year-old 501(c)3 nonpartisan nonprofit organization working to promote democratic values by shaping technology policy and architecture. The organisation is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

Authors

Lydia X. Z. Brown is a policy counsel with CDT's Privacy & Data Project, focused on disability rights and algorithmic fairness and justice. Their work has investigated algorithmic harm and injustice in public benefits determinations, hiring algorithms, and algorithmic surveillance that disproportionately impact disabled people, particularly multiply-marginalized disabled people. Outside their work at CDT, Lydia is an adjunct lecturer in disability studies and women's and gender studies at Georgetown University.

Ridhi Shetty is a policy counsel with CDT's Privacy & Data Project. Her work focuses on the relationship between equity, privacy, and data- and AI-driven practices in the public and private sector.

Matthew U. Scherer is Senior Policy Counsel for Workers' Rights and Technology Policy. He spearheads CDT's work on artificial intelligence, data, and other emerging tech issues in the workplace and labor market.

Andrew Crawford is a Senior Policy Counsel with CDT's Privacy & Data Project. His work centers around the privacy and equity implications of the collection, sharing, and use of health data.

Ableism And Disability Discrimination In New Surveillance Technologies

How new surveillance technologies in education, policing, health care, and the workplace disproportionately harm disabled people

Acknowledgements

We thank Ali*, Alma*, Brandy Mai, Courtney Bergan, David Burick, and Wiley Reading for sharing their stories with us. Much appreciation to CDT staff Alexandra Givens, Ari Goldman, Cody Venzke, Eric Null, Greg Nojeim, Hugh Grant-Chapman, Timothy Hoagland, and Samir Jain; disability rights/AI project advisory committee members Damien Patrick Williams, Karen Nakamura, and Rua M. Williams; and colleagues Corey Sauer, Cynthia L. Bennett, Jess L. Cowing, Os Keyes, and Shain A. M. Neumeier for their thoughtful comments and suggestions on this draft, as well as to Avatara Smith-Carrington for their early research on algorithms and risk and threat assessments.

* We did not use this person's real name at their request to protect their privacy.

May 2022

Table of Contents

Introduction 5

Educational Surveillance 7
Automated Virtual Proctoring 7
Automating Student Surveillance 14
Recommendations 25

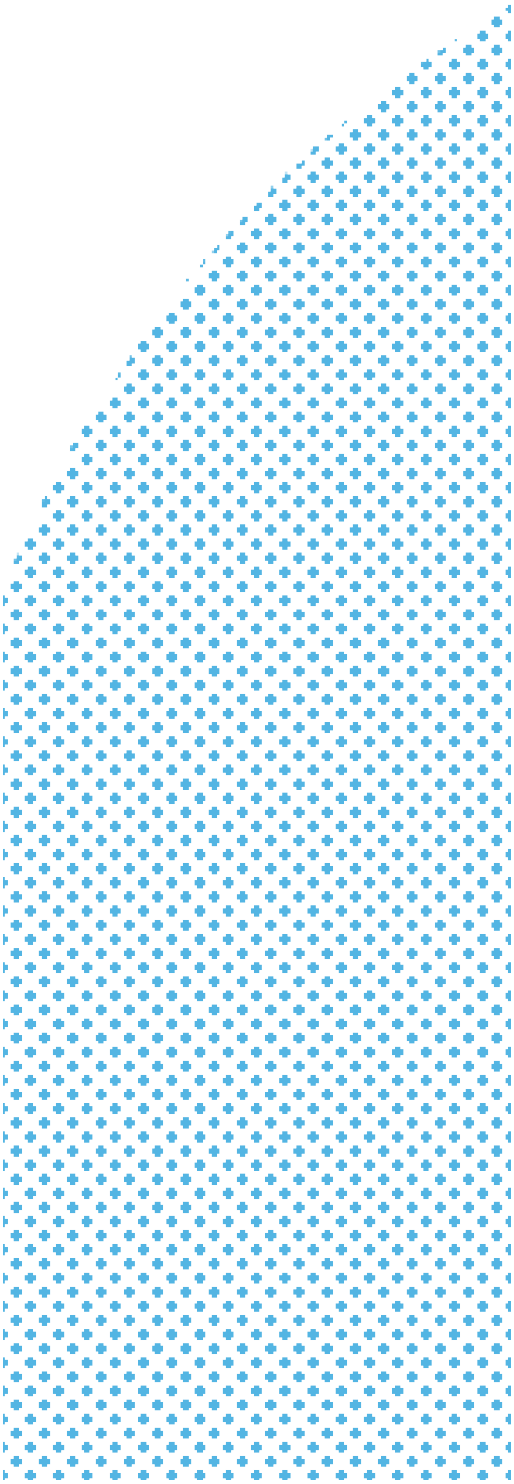
Criminal Legal System 26
Predictive Policing Software 27
Risk Assessment Algorithms 32
Use of Criminal Records in Tenant Screening Algorithms and Other Applications 34
Recommendations 38

Health Surveillance 40
Medications and Medical Devices That Track Compliance 43
Use of Predictive Analytics to Detect or Predict Likelihood of Mental Illness and Other Disabilities 44
Electronic Visit Verification Technology Adoption 46
Recommendations 49

Surveillance at Work 50
Algorithmic management and surveillance 50
Monitoring workers' health via employer-sponsored health and wellness programs 54
Recommendations 56

Conclusion 57

Introduction



Algorithmic technologies are everywhere. At this very moment, you can be sure students around the world are complaining about homework, sharing gossip, and talking about politics — all while computer programs observe every web search they make and every social media post they create, sending information about their activities to school officials who might punish them for what they look at. Other things happening right now likely include:

- Delivery workers are trawling up and down streets near you while computer programs monitor their location and speed to optimize schedules, routes, and evaluate their performance;
- People working from home are looking at their computers while their computers are staring back at them, timing their bathroom breaks, recording their computer screens, and potentially listening to them through their microphones;
- Your neighbors - in your community or the next one over - are being tracked and designated by algorithms targeting police attention and resources to some neighborhoods but not others;
- Your own phone may be tracking data about your heart rate, blood oxygen level, steps walked, menstrual cycle, and diet, and that information might be going to for-profit companies or your employer. Your social media content might even be mined and used to diagnose a mental health disability.

This ubiquity of algorithmic technologies has pervaded every aspect of modern life, and the algorithms are improving. But while algorithmic technologies may become better at predicting which restaurants someone might like or which music a person might enjoy listening to, not all of their possible applications are benign, helpful, or just.

Scholars and advocates have demonstrated myriad harms that can arise from the types of encoded prejudices and self-perpetuating cycles of discrimination, bias, and oppression that may result from automated decision-makers. These potentially harmful technologies are routinely deployed by government entities, private enterprises, and individuals to make assessments and recommendations about everything from rental applications to hiring, allocation of medical resources, and whom to target with specific ads. They have been deployed in a variety of settings including education and the workplace, often with the goal of surveilling activities, habits, and efficiency.

Disabled people[1] comprise one such community that experiences discrimination, bias, and oppression resulting from automated decision-making technology. Disabled people continually experience marginalization in society, especially those who belong to other marginalized communities such as disabled women of color. Yet, not enough scholars or researchers have addressed the specific harms and disproportionate negative impacts that surveillance and algorithmic tools can have on disabled people. This is in part because algorithmic technologies that are trained on data that already embeds ableist (or relatedly racist or sexist) outcomes will entrench and replicate the same ableist (and racial or gendered) bias in the computer system.[2] For example, a tenant screening tool that considers rental applicants' credit scores, past evictions, and criminal history may prevent poor people, survivors of domestic violence, and people of color from getting an apartment because they are disproportionately likely to have lower credit scores, past evictions, and criminal records due to biases in the credit and housing systems and in policing disparities.

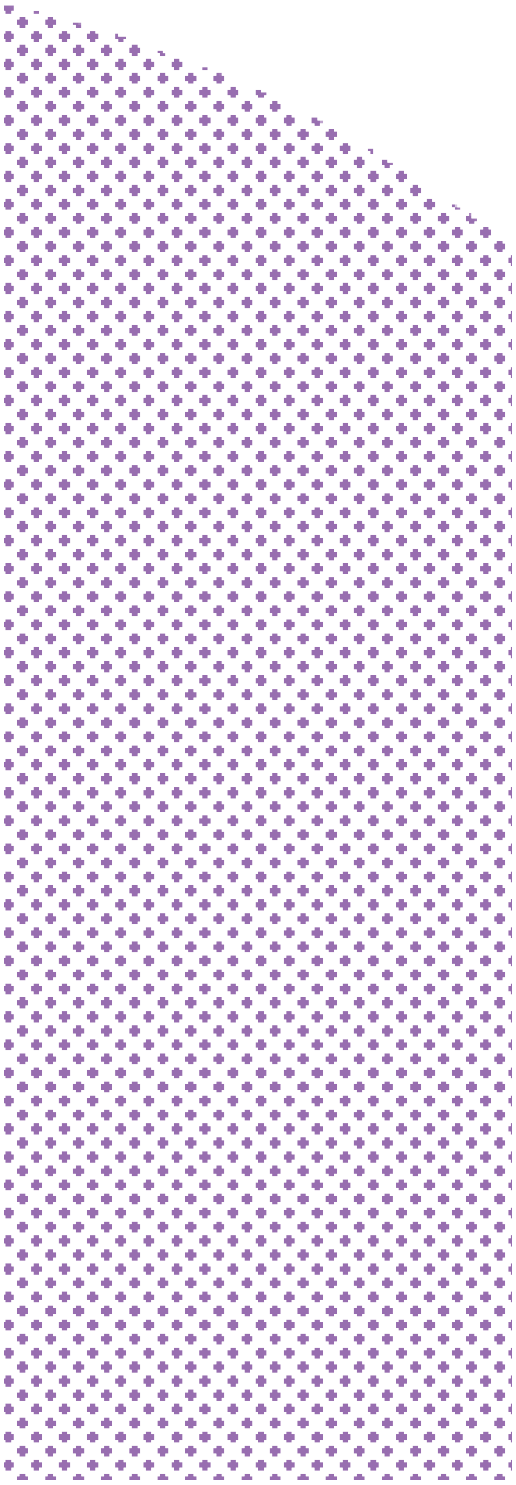
This report examines four areas where algorithmic and/or surveillance technologies are used to surveil, control, discipline, and punish people, with particularly harmful impacts on disabled people. They include: (1) education; (2) the criminal legal system; (3) health care; and (4) the workplace. In each section, we describe several examples of technologies that can violate people's privacy, contribute to or accelerate existing harm and discrimination, and undermine broader public policy objectives (such as public safety or academic integrity).

---

1 This report recognizes disability as a broad and culturally-informed category of identity and experience. Sins Invalid, a disability justice and performance art organization, defines disability as including "people with physical impairments, people who belong to a sensory minority, people with emotional disabilities, people with cognitive challenges, and those with chronic/severe illness. We understand the experience of disability to occur within any and all walks of life, with deeply felt connections to all communities impacted by the medicalization of their bodies." Our Mission & Vision, Sins Invalid, https://www.sinsinvalid.org/mission. Similarly, the U.N. Convention on the Rights of Persons with Disabilities defines disabled people as "those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others." United Nations Convention on the Rights of Persons with Disabilities, Article 1, https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-1-purpose.html.

2 Hayden Field, *An A.I. Training Tool Has Been Passing Its Bias to Algorithms for Almost Two Decades*, One Zero (Aug. 18, 2020), https://onezero.medium.com/the-troubling-legacy-of-a-biased-data-set-2967ffdd1035.

Educational Surveillance



Students face various forms of surveillance from early education through higher education, much of it intended to address two concerns: academic integrity and public safety. In recent years, schools have adopted technologically-augmented surveillance tools, some of which rely on predictive analysis and automated responses to flag suspicious behavior, trigger investigative or disciplinary action, or prioritize crisis response resources. The surveillance tools can have a disproportionate impact on disabled students and students of color - and likely on disabled students of color in particular.

Automated surveillance tools jeopardize students' privacy, dignity, and basic civil rights. In this section, we describe several types of educational surveillance tools, their impact on disabled students, and recommendations to address potential harms.

///

Automated Virtual Proctoring

Automated virtual proctoring is designed to replace an in-person proctor for testing and allow for test taking remotely. Instead of a human monitoring test-takers for suspicious behavior at the front of an in-person classroom, a software program on the test-taker's device (or, in some cases, a human watching a camera feed) conducts that monitoring. Given distance learning and the transmissibility concerns around COVID-19, automated and remote proctoring systems have become exponentially more widespread in both K-12 schools and higher education since the COVID-19

pandemic began.[3] Virtual proctoring largely takes two forms: automated virtual proctoring that relies on artificial intelligence and sophisticated machine learning systems; and people-based virtual proctoring that relies on granting strangers access to view students' home environments through a camera.[4]

Automated virtual proctoring systems are ostensibly designed to flag suspicious behavior that could indicate cheating, either by use of unauthorized materials, consulting with other people, or having another person take an exam instead of the actual student.[5] The systems attempt to prevent cheating by identifying atypical behaviors or rule violations. Software can use webcams, microphones, keyloggers, mouse tracking, and screen monitoring and recording to track students' movements, speech, activity, and input data. Students may not be allowed to speak out loud, have other people or animals present in the room, access other programs or the internet, or take unauthorized off-camera breaks.

Disabled students are more likely to be flagged as potentially suspicious either by a remote proctor or by remote proctoring AI systems simply because of the ways disabled people already exist and because of disability-specific access needs when test-taking.[6] The National Disabled Law Students Association raised many concerns about potential disability discrimination in a survey about remote proctoring for the 2020 bar exam.[7] Students noted that the behaviors flagged by or prohibited during automated proctoring are more likely to occur because of a disability, such as needing longer bathroom breaks or people who need to use screen readers or dictation software.[8] Additionally, the mere presence of the technology can cause or exacerbate anxiety, which is itself a disability.

---

3 Drew Harwell, *Mass School Closures in the Wake of the Coronavirus are Driving a New Wave of Student Surveillance*, Wash. Post (Apr. 1, 2020), https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/.

4 Elizabeth Laird, *Remote Proctoring of Exams is an Invasive Tool Without Clear Security Protections. States & Districts Should Avoid Rushing In*, The 74 (May 18, 2021), https://www.the74million.org/article/laird-remote-proctoring-of-exams-is-an-invasive-tool-without-clear-security-protections-states-districts-should-avoid-rushing-in/.

5 *Id.*

6 Lydia X. Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, Ctr. for Democracy & Tech. (Nov. 16, 2020), https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/; Shea Swauger, *Software That Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy*, MIT Tech. Rev. (Aug. 7, 2020), https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/; Shea Swauger, Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education, Hybrid Pedagogy (Apr. 2, 2020), https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/.

7 National Disabled Law Students Association, Report on Concerns Regarding Online Administration of Bar Exams 4-6 (2020), https://ndlsa.org/wp-content/uploads/2020/08/NDLSA_Online-Exam-Concerns-Report1.pdf.

8 *Id.* at 13-25.

***

Courtney Bergan is a neurodivergent white person with PTSD, Ehlers Danlos Syndrome, and low vision who took the Law School Admissions Test (LSAT) using ProctorU software. They shared this story:

"My experience was pretty awful in a variety of ways. I had accommodations for extended time along with breaks between sections to use the restroom, eat, take medications, etc. However, when I asked the remote proctor if I could use the restroom or get up to take my meds per my accommodations, I was told I could not and needed to remain in view of the camera. Not being able to use the restroom was pretty disruptive to my performance. By the time I got to the last section of the LSAT, I had to pee so badly that I was just clicking through answers trying to complete the test.

"I'm terrified to take other tests, including the [Multistate Professional Responsibility Exam] and Bar Exam, using this tech given my past experiences along with a congenital eye condition I have that causes uncontrolled eye movement, that I suspect will also get my test flagged."

Virtual proctoring software that incorporates facial detection and recognition technologies raises particular concerns for people of color and disabled people. Test administrators need to ensure that the person taking the test is the right person. To do this, they often use facial detection and recognition technologies that match the test taker to a photo. For example, one company requires students to look directly into their webcams to complete a "facial detection check," and then also uses facial recognition technology to determine "whether the person who started the exam switches to a different person along the way."[9]

It may also be harder for that technology to recognize people whose disabilities may affect their appearance or how easily they can engage with the technology. This could affect people with craniofacial conditions affecting bone structure, people who have had facial surgery, and people who use mobility devices, among others.[10] Similar bias could affect disabled people with conditions like ichthyosis, albinism, elephantiasis, or tumor growth that algorithms may not know how to interpret or recognize correctly. Further, one study found that blind and low vision people who had never before used biometric apps struggled to successfully take selfies to create a facial recognition database of blind subjects for biometrics, especially if conventional algorithms for facial detection and recognition were used.[11]

Because many facial recognition technologies are trained on biased data, they often do not represent people of color or disabled people sufficiently, which can lead to discrimination. Research has consistently shown that facial recognition technologies (which attempt to identify a specific person), and even mere facial detection (which attempts to detect whether any human face is present), are significantly less reliable and accurate on people of color, especially darker-complexioned people of color, than on white people.[12] The 2018 "Gender Shades" project showed that three well-known gender classification algorithms were significantly less accurate based on gender and skin tone, with error rates up to 34 percent higher for darker-skinned "females" than for lighter-skinned "males."[13] A 2019 assessment by the National Institute of Standards and Technology (NIST) confirmed these studies, finding that face recognition technologies across 189 algorithms are least accurate on women of

9 Class Action Compl. at ¶¶30, 71, Doe v. DePaul Univ., No. 2021CH01027 (Ill. Cir. Ct. Cook Cty., July 1, 2021), https://www.classaction.org/media/doe-v-depaul-university.pdf.

10 Sheri Byrne-Haber, *Disability and AI Bias*, Medium (July 11, 2019), https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533.

11 Norman Poh, Ramon Blanco-Gonzalo, Rita Wong & Raul Sanchez-Reillo, *Blind Subjects Faces Database*, 5 Inst. of Eng'g & Tech. Biometrics 20 (2016), https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-bmt.2015.0016.

12 It is well-known that FRT systems and other "intelligent" technology are trained on datasets that might themselves be biased or lack diversity. Beth Findley & Mariah Bellamoroso, *Why Racial Bias is Prevalent in Facial Recognition Technology*, J. L. Tech: JOLT Dig. (Nov. 3, 2020), https://jolt.law.harvard.edu/digest/why-racial-bias-is-prevalent-in-facial-recognition-technology.

13 Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proceedings of Machine Learning Research 2 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

color.[14] Because some communities of color have a higher prevalence of disability,[15] such discrimination will also have an outsized effect on disabled people of color.

Even as accuracy rates for race and gender increase, problems prevail. The most recent version of the NIST assessments, released in 2022, found significant improvements across the algorithms tested in recognition of women of color as compared to white men and white women.[16] But disability-related bias likely remains, given NIST's test does not incorporate disability-related bias, and facial recognition systems continue to be trained on datasets that do not represent disabilities. Even near-100 percent accuracy rates will still inaccurately identify tens, or potentially hundreds of thousands of people, leading to severe harm particularly in the areas discussed in this report.

Law school graduate Kiana Caton had to take matters into her own hands to mitigate this problem in facial recognition technology so that she could take her state bar exam, but this brought other unintended consequences:

> "[s]ometimes the light Kiana Caton is forced to use [to illuminate her face] gives her a headache. On top of common concerns that come with taking a state bar exam — like passing the test — Caton has to deal with challenges presented by facial recognition technology. She's a Black woman, and facial recognition tech has a well-documented history of misidentifying women with melanin. . . . To ensure her skin tone doesn't lead ExamSoft's remote test monitoring software to raise red flags, Caton will keep a light shining directly on her face throughout the two-day process, a tactic she picked up from fellow law school graduates with dark skin."[17]

Kiana is unable to take her test without being at a severe disadvantage introduced by the deficiencies of the proctoring technology. Having to endure many hours of a bright light that causes a headache will likely increase anxiety during the test as well as cause distracting pain, reducing her likelihood of passing – not because she doesn't know the material, but because the test-taking atmosphere is unreasonable.

Use of facial recognition technologies during remote proctoring might hinder accurate detection or identification of disabled students and students of color, leading to increased

---

14 Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Harv. U. Sci. in the News (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

15 Ctrs. for Disease Control & Prevention, Dept. of Health & Hum. Serv., Adults with Disabilities: Ethnicity and Race (last updated Sept. 16, 2020), https://www.cdc.gov/ncbddd/disabilityandhealth/materials/infographic-disabilities-ethnicity-race.html.

16 Nat'l Inst. of Standards & Tech., Ongoing Face Recognition Vendor Test: Part 1: Verification (2022), https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf.

17 Khari Johnson, *Examsoft's Remote Bar Exam Sparks Privacy and Facial Recognition Concerns*, Venture Beat (Sept. 29, 2020), https://venturebeat.com/2020/09/29/examsofts-remote-bar-exam-sparks-privacy-and-facial-recognition-concerns/.

risk of automated flagging and further scrutiny, while also increasing marginalized students' anxiety about the technology that in turn may negatively affect test performance.[18]

This type of bias has led to several legal challenges. The Electronic Privacy Information Center recently filed a civil rights complaint alleging that five remote proctoring companies violated students' privacy and engaged in unfair and deceptive trade practices.[19] The complaint enumerates three concerns about remote proctoring companies: (1) the collection of unnecessary and invasive details about students; (2) the use of undisclosed and unreliable algorithms to flag students for cheating; and (3) their deceptive claims about use of facial recognition technology and overall reliability of their systems.[20]

In another currently-pending case, *Gordon v. State Bar of California*, three disabled California law graduates sued the state bar after it refused to modify its remote proctoring protocols to accommodate their disabilities, instead insisting that they take the exam in person despite the severe health risks of the COVID-19 pandemic.[21] The *Gordon* plaintiffs sought accommodations from rules that made virtual proctoring effectively impossible for disabled test-takers. California's virtual system would not accommodate test takers who:

- were unable to stay in front of the web camera for the entirety of each test section, such as one disabled plaintiff who needed to take unscheduled bathroom breaks;
- needed a paper version of the exam, such as one disabled plaintiff who cannot use a computer screen for long periods of time;
- needed scratch paper, such as plaintiffs with ADHD;
- needed different amounts of extra time per test section; or
- used screen readers or dictation software.

In an effort to appease the bar administrators, plaintiffs offered to accept invasive and intrusive protocols, such as using Zoom on a second device to capture their workspace, explaining the need for an unscheduled break before taking one, and scanning their bathrooms with their web camera before use.[22] Test administrators would not accept these

18 See Letter from the ACLU Found. of N. Cal. to the Sup. Ct. of Cal. (Oct. 1, 2020), https://www.aclunc.org/sites/default/files/ACLU_Opp_to_Remote_Proctoring_CA_Bar_Exam_2020.10.01.pdf ("One Bar examinee, who is Arab-American, reports that he has attempted to verify his identity using ExamSoft's facial recognition system at least 75 times in several different rooms and with various lighting arrays, but has been unsuccessful. Another Bar examinee, who is a Black woman, reports that she plans to keep a light shining directly on her face for the duration of the two-day exam to prevent her skin tone from raising red flags." [internal citations omitted]).

19 Compl., In re Online Test Proctoring Companies (Dec. 9, 2020), https://epic.org/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf.

20 *Id.*

21 Compl., Gordon v. State Bar of California, No. 3:20-cv-06442 (N.D. Cal. Sept. 14, 2020), https://legalaidatwork.org/wp-content/uploads/2020/09/Gordon-v-State-Bar.pdf [hereinafter "Gordon Compl."].

22 *Id.* at ¶127(a)-(c).

terms, instead requiring disabled test takers to schedule an in-person exam despite higher risks of COVID-19 for disabled people. They imposed this requirement even though people with various disabilities have long been known to be at higher risk for COVID-19 infection and more severe experiences of the disease.[23] Other jurisdictions have continued to administer the bar exam using automated proctoring technologies up through at least February 2022.

Use of these systems may also violate the Americans with Disabilities Act (ADA) and related state disability nondiscrimination protections, as the ADA prohibits disability discrimination in federally-funded programs, services, and activities, as well as in places of public accommodation, covering nearly all K-12 educational settings as well as higher education institutions.[24]

The technology may also violate consumer protection law, such as the Illinois Biometric Information Privacy Act (BIPA).[25] Students at Northwestern and DePaul Universities sued their universities in 2021 alleging violations of BIPA. Both schools required students to install monitoring software on their computers for exam proctoring that collects vast amounts of information, "including facial recognition data, facial detection data, recorded patterns of keystrokes, eye monitoring data, gaze monitoring data, and camera and microphone recordings to effectively surveil students taking online exams."[26] Use of the automated proctoring software was mandatory to receive passing grades for courses. However, neither university told students what specific information they collected or offered a meaningful chance to opt out of the data collection. As of spring 2022, Northwestern students are currently awaiting a hearing on a motion to dismiss filed by the university, alleging that the school is not subject to requirements of the BIPA because it is statutorily exempt as a "financial institution."

---

23 *See* Ctrs. for Disease Control & Prevention, Dept. of Health & Hum. Serv., People with Certain Medical Conditions (last updated Feb. 25, 2022), https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-with-medical-conditions.html. These concerns are amplified for disabled people of color, who face compounded health disparities and higher risk during the pandemic because of racial and disability discrimination.

24 42 U.S.C. §§ 12132 and 12182; Unruh Civil Rights Act, Cal. Civ. Code § 51 (establishes right to "full and equal accommodations, advantages, facilities, privileges, or services in all business establishments of every kind whatsoever" regardless of disability, medical condition, genetic information and many other protected classes; incorporates federal Americans with Disabilities Act protections).

25 740 Ill. Comp. Stat. 14/15 (2008). BIPA requires informed written consent to collect, capture, use, store, and share biometric identifiers; prohibits disclosure or dissemination without consent unless required by law; and permanent destruction of such data after three years or once the purpose for collecting it has been satisfied, whichever comes first.

26 Compl., DePaul Univ., No. 2021CH01027, *supra* note 9, at ¶3; Class Action Compl. ¶3, Doe v. Nw. Univ., No. 2021CH00404 (Ill. Cir. Ct. Cook Cty., Jan. 27, 2021), https://s3.amazonaws.com/jnswire/jns-media/e0/c5/11521769/2021ch404.pdf.

Automating Student Surveillance

Students today are more likely to go online to study, socialize, and participate in community and political action. They are also more likely to face technology-enabled surveillance in their homes, on school-issued devices, and while in school or university buildings.

Automated surveillance is likely to have severe impacts for students with disabilities, who already face disproportionately high rates of school discipline and surveillance, and may need access to specific assistive and adaptive technology for their education. Disciplinary disparities are even worse for disabled students of color, with the National Council on Disability stating that "[r]acial and ethnic disparities in suspensions and expulsions suggest the presence of unconscious or implicit biases that combine with discrimination on the basis of disability to contribute to the School-to-Prison Pipeline crisis."[27] A recent CDT study of special education teachers and families of students with disabilities shows that they are similarly concerned about the use of automated student data to make decisions about students.[28] Of the special education teachers interviewed, 71% expressed concerns about schools using student data that reflects systemic bias to make decisions that could limit educational and workforce opportunities, and 64% expressed concerns about student data being shared with law enforcement.[29]

Amidst a backdrop of correlations between disproportionate discipline and future criminal legal system involvement, expansion of surveillance technologies in schools raises urgent concerns for students and advocates. These concerns are particularly prevalent when the technology is being used to conduct purported "threat assessments," monitoring students' social media, and activities on and off campus.

Threat Assessment

Schools are increasingly turning to automated software to expand threat assessment capabilities in the name of promoting public safety and preventing violence.[30] Today, software vendors like ALiCE, Crisis Go, and USA Software market behavioral threat assessment software that provides questionnaires and rubrics for school personnel to

---

27 Nat'l Council on Disability, Breaking the School-to-Prison Pipeline for Students with Disabilities 8 (2015) https://ncd.gov/publications/2015/06182015 (report available for download) [hereinafter Breaking the School-to-Prison Pipeline].

28 These elevated concerns are mirrored by family members of students with disabilities. Hugh Grant-Chapman, Ctr. For Democracy & Tech., *Tech for School Discipline? Parents and Teachers of Students with Disabilities Express Concerns* 2 (2022), https://cdt.org/insights/brief-tech-for-school-discipline-parents-and-teachers-of-students-with-disabilities-express-concerns/.

29 *Id.* These numbers compare to 58% of general education teachers and 44% of general education teachers respectively.

30 Priyam Madhukar, *The Hidden Costs of High-Tech Surveillance in Schools*, Brennan Ctr. for Just. (Oct. 17, 2019), https://www.brennancenter.org/our-work/analysis-opinion/hidden-costs-high-tech-surveillance-schools.

Automated surveillance is likely to have severe impacts for students with disabilities, who already face disproportionately high rates of school discipline and surveillance, and may need access to specific assistive and adaptive technology for their education.

follow, as well as predictive data analytics, in determining whether students pose a threat.[31] The threat assessment process may ask human evaluators to consider a person's appearance, apparent interests, and friendships or associations.[32] Additionally, OnGuard markets a school safety package consisting of four surveillance programs that, among other features, monitor students' personal social media posts using location data, machine learning, and keyword screening.[33] These programs are meant to be used in conjunction with a team of human reviewers conducting a threat assessment, who are supposed to consider multiple factors, including context, when a student or incident comes to their attention. Because there is often overlap between disability and race, we cover the impacts of threat assessment on both.

Threat assessment poses a high risk of disproportionate impact on disabled students and students of color, who may be more likely to be referred to threat assessment teams. While some research indicates that threat assessment

31 *See, e.g., School Threat Assessment Software for Students*, ALICE Training, https://www.alicetraining.com/our-program/threat-assessment-software/; *Student Threat Assessment Manager*, CrisisGo, https://www.crisisgo.com/student-threat-assessment-manager; *Behavioral Threat Assessment and Case Management System*, USA Software, Inc., https://threatassessmenttracking.com.

32 Model Behavioral Threat Assessment Policies and Best Practices for K-12 Schools, Florida Department of Education Office of Safe Schools, Jul. 2021, https://www.fldoe.org/core/fileparse.php/19958/urlt/8-5.pdf%20 (mentions changes in appearance or habits as concerning behavior that may or may not be a threat but could require intervention); Threat Assessment Plan, Ventura County Office of Education, Jan. 2018, https://www.vcoe.org/LinkClick.aspx?fileticket=7edHzHCPS14%3D&portalid=7 (mentions "deteriorating physical appearance and self-care" as a warning sign of potentially violent behavior).

33 Andrew Westrope, *School Safety Package Includes AI, Social Media Monitoring*, Gov't Tech. (Aug. 22, 2019), https://www.govtech.com/biz/school-safety-package-includes-ai-social-media-monitoring.html.

teams manage to avoid racial bias at a superficial level,[34] other research shows that students with disabilities are more likely to be referred to threat assessment than nondisabled students, and that schools with higher populations of students of color are more likely to use threat assessment teams.[35] Additionally, once students are flagged, human reviewers and automated language analysis alike might misinterpret or criminally profile speech patterns, slang, and perceived or observed interests or activities that might be associated with specific disabilities and minoritized cultures. This could negatively affect students who have perceived antisocial tendencies or "inappropriate" tone because they are neurodivergent, or who use Black American English/African American Vernacular English. Those students with disabilities or Black students would then be more likely to be misunderstood or subjected to unjust profiling, leading to discipline and harsher punishment. Additionally, those with racially biased perceptions of disabilities, such as schizophrenia, may interpret benign actions of disabled Black people as violent or aggressive.[36]

Student threat monitoring can exacerbate and accelerate complaints driven by disability prejudice and discrimination, particularly fears that mental health disabilities or developmental disabilities are predictors for violence. Such examples are readily identifiable in the cases of a white autistic high school student in Oregon profiled as a would-be school shooter in the absence of making any actual threat,[37] and a Black autistic elementary school student in New Mexico referred for threat assessment after having a meltdown in which he

34 Audrey Breen, *Study: K-12 Threat Assessment Teams Prove Effective, Without Racial Bias*, UVA Today (Mar. 17, 2016), https://news.virginia.edu/content/study-k-12-threat-assessment-teams-prove-effective-without-racial-bias (citing research led by Dewey Cornell, Virginia Youth Violence Project, in conjunction with the state Department of Criminal Justice Services and Department of Education, that found no racial disparities in disciplinary outcomes for white, Black, and Hispanic students referred to the threat assessment process).

35 Stephen Sawchuk, *What Schools Need to Know About Threat Assessment Techniques*, Ed. Week (Sept. 3, 2019), https://www.edweek.org/leadership/what-schools-need-to-know-about-threat-assessment-techniques/2019/09 ("Federal data also display some patterns worth noting. Schools with higher proportions of nonwhite students were more likely than those with fewer students of color to report using threat assessment teams."); Dewey Cornell & Jennifer Maeng, Nat'l Crim. Just. Reference Serv., Student Threat Assessment as a Safe and Supportive Prevention Strategy: Final Technical Report 24 (2020) https://www.ojp.gov/pdffiles1/nij/grants/255102.pdf ("students receiving special education services were 3.9 times more likely to be referred for threat assessment than those not receiving special education services [and t]he proportion of Black students referred for threat assessment was 1.3 times higher than the proportion of White students"); Jazmyne Owens, New America, Threat Assessment Systems as a School Safety Strategy (2021), https://www.newamerica.org/education-policy/briefs/threat-assessment-systems-as-a-school-discipline-safety-strategy/ (describes "disproportionate identification of students with disabilities and students of color" as a civil rights concern identified in Cornell and Maeng's research).

36 This idea has persisted for decades despite its basis in racism and its scientific inaccuracy. Jonathan M. Metzl, *The Protest Psychosis: How Schizophrenia Became a Black Disease* (Beacon Press, 2010), x-xi; xiv-xvi.

37 Bethany Barnes, *Targeted: A Family and the Quest to Stop the Next School Shooter*, The Oregonian/OregonLive, (Aug. 29, 2019), https://www.oregonlive.com/news/erry-2018/06/75f0f464cb3367/targeted_a_family_and_the_ques.html.

bit and hit a teacher.[38] In the latter student's district, disabled students were 56% of all threat assessments for the previous year, even though they comprised only 18% of the student population.[39] Additionally, such monitoring could also lead to or exacerbate racial and religious profiling, such as that in programs like Countering Violent Extremism and locally-based programs that disproportionately target Black and Latinx youth for gang operations and Arab and South Asian Muslim youth for counterterrorism and undercover operations.[40] For instance, in separate studies, 28% of Muslim students in New York City public schools reported being racially profiled and stopped by police, while 28% of Muslim high school students in California public schools reported discrimination by a teacher or administrator.[41] Likewise, Black students represented 9.6% of threat assessment subjects, but only 2.6% of the overall student population.[42] Religious and racial profiling can contribute to mental health distress in students from marginalized religious and racial communities.

Social Media and Off-Campus Monitoring

Schools have increasingly turned to automated analysis of social media content and other online activity as a way to predict potential threats of violence or otherwise invoke

38 Ike Swetlitz, *When Kids Are Threats: The Assessments Unfairly Targeting Students With Disabilities*, The Guardian, (Oct. 15, 2019), https://www.theguardian.com/us-news/2019/oct/14/when-kids-are-threats-the-assessments-unfairly-targeting-students-with-disabilities.

39 *Id.*

40 *See* Faiza Patel, *Ending the 'National Security' Excuse for Racial and Religious Profiling*, Brennan Ctr. for Just. (July 22, 2021), https://www.brennancenter.org/our-work/analysis-opinion/ending-national-security-excuse-racial-and-religious-profiling; *#StopCVE*, www.stopcve.com; Brennan Ctr. for Just., *Countering Violent Extremism (CVE): A Resource Page*, https://www.brennancenter.org/our-work/research-reports/countering-violent-extremism-cve-resource-page (last updated Oct. 4, 2018); Emily Galvin-Almanza, *California Gang Laws are Normalized Racism*, The Appeal (Oct. 4, 2019), https://theappeal.org/drakeo-california-gang-laws-racism/; John Tarleton, *NYPD Spy Scandal Hits CUNY: Muslim Students Target of Profiling*, Clarion (CUNY Prof. Staff Cong., New York, N.Y.), Nov. 2011, https://www.psc-cuny.org/clarion/november-2011/nypd-spy-scandal-hits-cuny-muslim-students-target-profiling.

41 Louis Cristillo, Teachers College Colum. U., Religiosity, Education and Civic Belonging: Muslim Youth in New York City Public Schools 12 (2008), https://www.tc.columbia.edu/i/media/6581_musnycreport.pdf; The Council on American-Islamic Relations (CAIR) California, Mislabeled: The Impact of School Bullying and Discrimination on California Muslim Students 18 (2017) http://web.archive.org/web/20171201040632/https://ca.cair.com/sfba/wp-content/uploads/2015/10/CAIR-CA-2015-Bullying-Report-Web.pdf (accessed via Wayback Machine on May 18, 2022).

42 Ike Swetlitz, *When Kids Are Threats: The Assessments Unfairly Targeting Students With Disabilities*, The Guardian, (Oct. 15, 2019), https://www.theguardian.com/us-news/2019/oct/14/when-kids-are-threats-the-assessments-unfairly-targeting-students-with-disabilities.

disciplinary authority.[43] Use of this technology is common. Recent CDT research found that 81% of K-12 teachers reported that their school uses some form of student activity monitoring software, and of this group, 43% report that monitoring software is used for disciplinary purposes.[44] As a result of this surveillance, marginalized students face increased scrutiny from school administrators, putting them at greater risk when algorithms flag for discipline their voices, appearances, and social media content at higher rates than nondisabled and white students.

An increasing number of safety management platforms offer monitoring services, yet research shows that automated social media monitoring software lacks nuance and discretion to interpret or respond to dynamic content.[45] Some software relies on the use of a static, preset list of keywords to be flagged as suspicious or threatening.[46] This means that if a student writes, "I bombed that biochem exam," "shoot, I forgot my backpack," or even "researching arguments for and against private gun ownership for self-defense," they might automatically face scrutiny as a security threat, despite the clear absence of threatening content in these examples.[47]

---

43 *See, e.g., Tools for School Safety in K-12*, Kidio, https://kid.io/school_safety_platform/; Digital Mgmt., Inc. (DMI), *DMI Arms Teachers, Students, Parents and Schools with Mobile Phones, Real-Time Security App*, Globe Newswire (Mar. 20, 2018), https://www.globenewswire.com/en/news-release/2018/03/20/1442660/0/en/DMI-Arms-Teachers-Students-Parents-and-Schools-with-Mobile-Phones-Real-Time-Security-App.html; Rekor Systems, Inc., Rekor *Launches OnGuard Comprehensive School Safety Program to Enhance Student Safety Nationwide; First Implementation to Be in Upstate New York*, Accesswire (Aug. 6, 2019), https://www.accesswire.com/554724/Rekor-Launches-OnGuard-Comprehensive-School-Safety-Program-to-Enhance-Student-Safety-Nationwide-First-Implementation-to-be-in-Upstate-New-York; *How We Help Protect Your Kids*, Bark, https://www.bark.us/schools; *Save Lives By Detecting Warning Signs of Suicide, Cyberbullying, and School Violence*, Lightspeed Alert, https://www.lightspeedsystems.com/solutions/lightspeed-alert/.

44 Elizabeth Laird & Hugh Grant-Chapman, Ctr. for Democracy & Tech., Navigating the New Normal: Ensuring Equitable and Trustworthy EdTech for the Future 4 (2021), https://cdt.org/insights/report-navigating-the-new-normal-ensuring-equitable-and-trustworthy-edtech-for-the-future/.

45 *See generally* Hannah Quay-de la Vallee & Natasha Duarte, Ctr. for Democracy & Tech., Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data 10-13 (2019), https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/.

46 Aaron Leibowitz, *Could Monitoring Students on Social Media Stop the Next School Shooting?*, N.Y. Times (Sept. 6, 2018), https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html.

47 Quay-de la Vallee, *supra* note 45.

***

Ali (not their real name) is a disabled student of color who was targeted for surveillance, profiling, and discriminatory discipline by university administration and other students. They shared this story:

"It started when I stood up to bigoted preachers. One person fabricated that I was planning to stalk and take out a lecturer. I was angry because he tried to get sexually involved with a student, but I wasn't even planning to confront him. Things I said were taken out of context.

Other students were stalking me digitally, possibly working together or with university administrators. Sometimes they pretended to be my friends, getting me to vent about mistreatment, wishing I had payback, and taking fake 'evidence' of me threatening people in ways I wouldn't actually do, based on my posts about politics and cops.

One time someone joked that if I got removed from on-campus residence, I should go out 'with a bang,' meaning a loud party with vodka on the floor, paint on the walls, trash on fire. I thought it was hilarious so I made a joke too. Then I was accused of threatening to burn down the building.

Other students monitored my social media as I got into first-person shooter games and followed Instagram accounts with gun photos. They were looking for anything. I sent a gym selfie and one accuser said I was working out to fight someone. I made one offhand comment about missing an old friend because I saw them on campus near my residence, and I got accused of stalking. I lost a bunch of friends to rumors.

The university fought against sharing all the evidence even when lawyers got involved. I got trumped up disciplinary charges with no proof for any of them. I had a private hearing with an appeals committee to reverse a de facto expulsion. My hearing actually succeeded even though I'm banned from campus for 'trespassing' for a couple years. I transferred to another school."

Other software uses more complex language processing and machine learning to interpret students' posts, but can still fail to accurately interpret or assess the content of those posts. That risk is especially high for students from marginalized communities or who are not fluent in or using standard English, a particular concern for many disabled people whose disabilities and cultures affect language. For example, one study found that AI programs looking for hate speech were 1.5 times "more likely to flag tweets as offensive or hateful when they were written by African Americans, and 2.2 times more likely to flag tweets written in African American English."[48] Another study found that when *people* were asked to identify hate speech, they almost always disagreed – only 5% of tweets in the study using words from a hate speech lexicon were labeled hate speech by a majority of participants, and only 1.3% were unanimously labeled hate speech.[49] And since people also write the AI programs and respond to their output, their biases will affect an AI's baseline understanding of what constitutes hate speech as well as how the AI systems are used.

As described above with facial recognition software, monitoring software in this context also learns to make decisions based on existing information and data sets. If existing data sets already reflect racial, gender, or disability bias, then the algorithmic systems will replicate and reinforce those very same biases. For example, if students and teachers have reported more posts from Black, Muslim, or disabled students as potentially suspicious or threatening, then a software program might learn to assign a higher level of risk to posts made by students who share those characteristics - and then teachers and administrators might be more likely to perceive students from those groups as problems.

Additionally, as more students rely on school-issued devices during the pandemic, schools are surveilling an increasing number of disproportionately lower-income students who use such devices, with 71% of K-12 teachers reporting that their school or district uses student activity monitoring software on school-issued devices, while only 16% report that it is used on family-owned devices.[50] This surveillance may look for potential predictors of violence

---

48 Shirin Ghaffary, *The Algorithms That Detect Hate Speech Online Are Biased Against Black People*, Vox (Aug. 15, 2019), https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter (citing Maarten Sap et al., The Risk of Racial Bias in Hate Speech Detection, Proc. of the 57th Ann. Meeting of the Ass'n for Computational Linguistics 1668, 1670-71 (2019), (https://aclanthology.org/P19-1163.pdf)). *See also* Natasha Duarte & Emma Llansó, Ctr. for Democracy & Tech., Mixed Messages? The Limits of Automated Social Media Content Analysis 15-19 (2017), https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/ (discussing extreme unreliability of automated social media content analysis for detecting future terroristic activity, differentiating between sarcasm and jokes, or distinguishing between meanings in different cultural and situational contexts, especially for marginalized communities).

49 Thomas Davidson et al., *Automated Hate Speech Detection and the Problem of Offensive Language*, 11 Proc. Eleventh Int'l AAAI Conf. on Web and Soc. Media 512, 513 (2017), https://ojs.aaai.org/index.php/ICWSM/article/view/14955/14805.

50 DeVan L. Hankerson, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman & Dhanaraj Thakur, *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software*, Center for Democracy and Technology 6-7 (2021) https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/.

or even of self-harm and suicide, leading to increased scrutiny, potentially inappropriate interventions, and possible profiling.[51]

Yet, merely adding a layer of human review to social media monitoring does not remove embedded bias from these systems, as racism and ableism in schools are well documented.[52] The African American Policy Forum's Kimberlé Williams Crenshaw notes, for instance, that during the 2011-2012 school year, "Black girls in New York were nearly ten times more likely to be suspended than their white counterparts."[53] Since then, nationally, disabled students were arrested nearly three times more than nondisabled students, made up 80% of all students physically restrained in schools, and represented up to 85% of youth incarcerated in juvenile prison.[54] (Current statistics are hard to find, and extant statistics may use inconsistent definitions of disability.)

On-Campus Surveillance

In the effort to increase campus safety, schools now use a variety of on-site surveillance technologies in addition to the widespread use of metal detectors and in-school or on-campus police. These technologies include aggression-detection microphones and facial recognition technology used to identify people and their movements and associations.[55]

---

51 Sara Collins, Jasmine Park, Anisha Reddy, Yasamin Sharifi & Amelia Vance, *The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies*, Student Privacy Compass (2021), https://studentprivacycompass.org/resource/self-harm-monitoring/.

52 Office of Civil Rights, U.S. Dept. of Ed., 2015-16 Civil Rights Data Collection: School Climate and Safety (2018), https://www2.ed.gov/about/offices/list/ocr/docs/school-climate-and-safety.pdf (revised May 2019) (illustrating the breakdown of school discipline and law enforcement referral by race, gender, and disability); U.S. Gov't Accountability Office, GAO-18-258, Discipline Disparities for Black Students, Boys, and Students with Disabilities (2018) https://www.gao.gov/assets/gao-18-258.pdf (comparing the discipline of Black students with disabilities to disabled students of other races).

53 Kimberlé Williams Crenshaw, Priscilla Ocen & Jyoti Nanda, African Am. Pol. F. & Ctr. for Intersectionality and Soc. Pol. Stud., Black Girls Matter: Pushed Out, Overpoliced, and Underprotected 24 (2015), https://44bbdc6e-01a4-4a9a-88bc-731c6524888e.filesusr.com/ugd/b77e03_e92d6e80f7034f30bf843ea7068f52d6.pdf ("in Boston, [Black girls] were suspended at almost twelve times the rate of white girls. In New York, Black boys were suspended at a rate five times that of white boys. In Boston, Black boys were 7.4 times more likely to be suspended than their white counterparts").

54 Daja E. Henry & Kimberly Rapanut, *How Schools and the Criminal Justice System Both Fail Students With Disabilities*, Slate (Oct. 21, 2020, 9:00 AM), https://slate.com/news-and-politics/2020/10/students-disabilities-criminal-justice-system.html (citing data from the 2015-2016 school year and explaining how Black students are more often punished for behaviors associated with their disabilities); U.S. Dept. of Ed., 2017-2018 Civil Rights Data Collection: The Use of Restraint and Seclusion on Children with Disabilities in K-12 Schools 6 (2020), https://www2.ed.gov/about/offices/list/ocr/docs/restraint-and-seclusion.pdf (stating that in 2017-2018, disabled students made up 80% of all students subjected to physical restraint and 78% of all students subjected to restraint or seclusion); Breaking the School-to-Prison Pipeline, *supra* note 27, at 5 (reporting in 2015 that "up to 85 percent of youth in juvenile detention facilities have disabilities that make them eligible for special education services").

55 Madhukar, *supra* note 30. Schools also use vehicle recognition software and automatic license plate readers. *Id.*

These technologies are meant to identify unauthorized visitors - and sometimes to analyze "affect" (tone, emotion, or attitude) - but can result in tracking information about students and staff, and potentially replicate existing patterns of racial, gender-based, and disability-based discrimination.[56]

Aggression-detection microphones purport to use machine learning software to detect distress, aggression, anger, fear, or duress in voices. If the microphones detect targeted noise over a certain threshold, the software sends an immediate alert to designated school personnel with the nature and location of the targeted noise. The school employees can then decide whether or how to intervene. For example, the software is meant to pick up on someone screaming in fear, yelling a threat, or engaging in a verbal altercation. These audio analysis technologies are used not only in schools, but also in hospitals and prisons.[57]

Aggression-detection microphones and affect recognition technology raise concerns about gender, disability, and racial profiling in determining which students should be flagged as potentially aggressive. These technologies could particularly impact autistic students, deaf students, and students with cerebral palsy who may have difficulty modulating voice volume, as well as students with mental health disabilities and learning disabilities who express anger and frustration without actual intent to engage in violence toward others. Additionally, the technology is already fairly inaccurate; a ProPublica analysis identified hundreds of false positives from aggression-detection devices for ordinary and non-threatening sounds, including laughing, coughing, and closing locker doors, which raises concerns for students with vocal tics, impulsivity, and atypical speech due to disabilities like Tourette's, cerebral palsy, and ADD.[58]

Much like the systems discussed above, systems that use facial recognition technology to identify whether a person is supposed to be on school property risk misidentifying both disabled students and students of color because of the known accuracy flaws of the technology. University of Michigan researchers cautioned that they:

> "...expect FR [facial recognition] in schools to target and harm vulnerable students: for example, FR is likely to increase the frequency with which Black and brown

---

56 John S. Cusick & Clarence Okoh, *Why Schools Need to Abandon Facial Recognition, Not Double Down On It*, Fast Company (Jul. 23, 2021), https://www.fastcompany.com/90657769/schools-facial-recognition.

57 *See, e.g.*, Sara Mosqueda, *Audio and Acumen Against Aggression*, Security Mgmt. (ASIS Int'l, Alexandria, V.A.), Mar. 1, 2021, https://www.asisonline.org/security-management-magazine/articles/2021/03/audio-and-acumen-against-aggression/; Rochisha Shukla, Bryce E. Peterson, Lily Robin & Daniel S. Lawrence, Audio Analytics and Other Upgrades in Correctional Surveillance Systems: Lessons Learned from Two Minnesota Facilities, Urban Inst. (2021), https://www.urban.org/sites/default/files/publication/103620/audio-analytics-and-other-upgrades-in-correctional-surveillance-systems-lessons-learned-from-two-minnesota-facilities_0.pdf.

58 Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.

students are singled out and disciplined by school administrators. Also, because FR has higher error rates for Black and brown subjects, it is likely to malfunction for students of color more often than their white counterparts. This could have the effect of further excluding and victimizing already marginalized students."[59]

These fears were borne out in early 2020 when a school in the Lockport City School District in upstate New York became the first in the United States to adopt facial recognition software as a public safety measure intended to prevent a mass shooting.[60] Less than a year later, investigative journalists uncovered that the private vendor selling the software had lied about the accuracy and reliability of its software, which mistook broom handles for guns and was four times more likely to misidentify a Black man than a white man, and 16 times more likely to misidentify a Black woman than a white man.[61] These astoundingly high error rates on basic information (object identification) and racially biased inaccuracies raise further questions about the reliability of facial recognition software in identifying disability-related objects (like canes, crutches, or oxygen tanks) or disabled people's bodies.

Additionally, surveillance technologies may fail to detect or prevent any actual signs of imminent violence. This is both because of the relative rarity of school shootings (compared to other types of violence in schools) and, in the case of facial recognition technologies, the even lower likelihood that such violent acts are carried out by strangers to the school. Of course, school shootings are horrific acts of violence that require proactive response and preventative strategies. But automated mass surveillance measures are not only ineffective at preventing such violence, but unjustifiably intrusive and harmful in and of themselves.

59 Claire Galligan, Hannah Rosenfeld, Molly Kleinman, & Shobita Parthasarathy, *Cameras in the Classroom: Facial Recognition Technology in Schools: Technology Assessment Project Report*, Science, Technology and Public Policy at the University of Michigan (2020) at 30 https://stpp.fordschool.umich.edu/sites/stpp/files/uploads/file-assets/cameras_in_the_classroom_full_report.pdf.

60 *Id*. at 53-54.

61 Todd Feathers, *Facial Recognition Company Lied to School District About its Racist Tech*, Vice: Motherboard (Dec. 1, 2020), https://www.vice.com/en/article/qjpkmx/fac-recognition-company-lied-to-school-district-about-its-racist-tech; Gonzague Rolland, *Facial Recognition and Racist Algorithm in Schools: Costly Fiasco in New York State*, CTRLZ Mag. (Feb. 12, 2021), https://ctrlzmag.com/facial-recognition-and-racist-algorithm-in-schools-costly-fiasco-in-new-york-state/.

Recommendations

- **Prior to purchasing, and when designing or implementing an automated, "intelligent" system for tracking or monitoring students, consult with and center the recommendations of disabled people (and other marginalized communities)** to help ensure the system does not discriminate against or otherwise cause them harm, and analyze (with external audits) the software to ensure it achieves its goal.
- **After purchasing, frequently assess the software** to ensure that it is not discriminating against marginalized communities.
- **Be transparent, clear, and flexible when implementing these systems, and educate parents and students about their use and their potential consequences,** including how the school has attempted to mitigate any bias built into the system.
- **Schools should recognize that requesting accommodations is often difficult and it takes a toll on disabled students.**
  - » Schools should make clear that students with disabilities may request accommodations and that the process will be easy, and that those requests will be met with judgment-free and empathetic responses (which might require administrator training).
  - » Schools should also make common forms of accommodations freely available.
- **Schools should not force students to accept constant surveillance.**
  - » Schools should explain the nature of the tracking and monitoring products.
  - » Schools should give students and their families a choice about whether to participate.
  - » Schools should allow for opting out of systems that are invasive or intrusive.
  - » Schools should provide students with webcam shutters.
- **The Department of Justice and Department of Education should issue updated guidance** clarifying that nondiscrimination, reasonable accommodations, and manifestation determination provisions of Title II of the Americans with Disabilities Act, Section 504 of the Rehabilitation Act, and the Individuals with Disabilities Education Act apply to school discipline and monitoring brought on by tech platforms.

Criminal Legal System

As with other public and private actors, police, prosecutors, courts, and prisons have increasingly turned to technological solutions to streamline operations and focus resources. Recent decades have witnessed a vast expansion of surveillance technologies that have further deepened the problem of mass incarceration and its collateral consequences. Police departments use software to predict where crime will happen and who will commit crimes, and judges rely on algorithms to evaluate which defendants should be released on bail. These uses have downstream consequences beyond intensified policing and incarceration. For instance, some landlords have automatically disqualified rental applicants based on records of conviction, and even based on arrest records that don't indicate whether the person was even convicted. This can affect a person's rental prospects and housing stability.

Most research, reporting, and advocacy around automated tools for criminalization and incarceration has focused exclusively on the racist impact of these tools.[62] Increasingly, advocates have also named the importance of gender, class, and faith-based discrimination and marginalization in AI-driven criminalization.[63] Yet, these tools also present disproportionate risks to disabled people because of characteristics more likely to be considered in predictive

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

63 *See, e.g.*, Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. 192, 218-23 (2019), https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf (discussing confirmation feedback loop impacting transgender people targeted for hyper criminalization by New Orleans Police Department, and majority non-white and low-income neighborhoods experiencing heightened policing resulting from gentrification).

policing programs and risk assessment algorithms.[64]

Ultimately, predictive policing software and algorithmic risk assessments reinforce discrimination and disproportionate criminalization because of data proxies for racial and socioeconomic class, which also often function as proxies for disability.[65]

Predictive Policing Software

Use of predictive policing analytics to enable and expand policing practices that are racially-biased - and thus likely also biased against many disabled people - is not a new phenomenon. In 1994, the New York Police Department adopted the CompStat data management system that has since grown into a predictive policing tool, pressuring officers to increase the numbers of stops they make, and enabling officers to instantly access data and analytics about arrests, criminal histories, and parole and probation information.[66] In the decades since, law enforcement agencies have increasingly adopted predictive policing data analytics tools and biometric surveillance technologies, including advanced facial recognition software, to allocate resources and target specific types of crime and communities.[67]

For example, the Los Angeles Police Department (LAPD) notoriously used two algorithmic programs to target particular individuals and communities for greater policing. Beginning in 2008, LAPD started developing a program called Operation LASER (Los Angeles Strategic Extraction and Restoration), which used an algorithm to identify "chronic offenders" based on a points system: a person would gain points for factors like being on parole or probation, having a gang designation (many of which are notoriously inaccurate), or being stopped on

64 Lydia X. Z. Brown & Ridhi Shetty, *Critical Scrutiny of Predictive Policing is a Step to Reducing Disability Discrimination*, Ctr. for Democracy & Tech. (July 23, 2020), https://cdt.org/insights/critical-scrutiny-of-predictive-policing-is-a-step-to-reducing-disability-discrimination/.

65 *See generally* Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1258 (2020), https://ilr.law.uiowa.edu/assets/Uploads/ILR-105-3-Prince-Schwarcz-6.pdf.

66 Chris Smith, *The Controversial Crime-Fighting Program That Changed Big-City Policing Forever*, N.Y. Mag.: The Intelligencer (Mar. 2018), https://nymag.com/intelligencer/2018/03/the-crime-fighting-program-that-changed-new-york-forever.html.

67 Maya Ahmed, *Aided by Palantir, the Lapd Uses Predictive Policing to Monitor Specific People and Neighborhoods*, The Intercept (May 11, 2018), https://theintercept.com/2018/05/11/predictive-policing-surveillance-los-angeles/ (citing Stop LAPD Spying Coalition, Dismantling Predictive Policing in Los Angeles (2018), https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf).

foot or in a traffic stop.[68] The department also used an algorithm to predict locations where the department expected higher crime rates, so they could target those locations for greater policing.[69] The program enabled coordination between LAPD and the municipal prosecutors' office, as well as the city attorney's nuisance abatement program, even leading to police pressure on landlords to increase surveillance at their properties or evict specific tenants.[70] An inspector general's audit described Operation LASER as "analogous to laser surgery ... to remove tumors."[71]

Similarly, Chicago piloted a person-based program in 2013 that used data from people's arrest records and social networks to assess their risk of involvement in shootings.[72] The civil rights organization Upturn found that one-third of people included on the resulting "Strategic Subject List" had no history as perpetrators or victims of any crime.[73] Even worse, Upturn found that mere inclusion on the list for any reason was a predictor of future arrests, in a self-fulfilling prophecy.

The LAPD's original programs were finally shuttered in 2019 and 2020 after extensive legal challenges, including public concerns that the programs encoded existing racial, class, and other biases about where police believe criminal activity will happen.[74] Similarly, Chicago

68 Dismantling Predictive Policing in Los Angeles, *supra* note 67, at 10-11. *See also*, Dan Hinkel, *CPD Has Made Little Progress on Vow to Replace Gang Database Criticized as Error-Filled and Racially Discriminatory, City Watchdog Says*, Chi. Trib. (Mar. 31, 2021, 5:51 PM), https://www.chicagotribune.com/news/breaking/ct-chicago-police-gang-database-inspector-general-report-20210331-vor2twpvzbdxthai5qikpbekjy-story.html; Emmanuel Felton, *Gang Databases Are a Life Sentence for Black and Latino Communities*, Pac. Standard (Mar. 15, 2018), https://psmag.com/social-justice/gang-databases-life-sentence-for-black-and-latino-communities.

69 Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Justice (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

70 Stop LAPD Spying Coalition, Stop LAPD Spying Coalition Wins Groundbreaking Public Records Lawsuit, Medium (Dec. 9, 2019), https://stoplapdspying.medium.com/stop-lapd-spying-coalition-wins-groundbreaking-public-records-lawsuit-32c3101d4575.

71 Mark Puente, *LAPD Ends Another Data-Driven Crime Program Touted To Target Violent Offenders*, L.A. Times (Apr. 12, 2019), https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html.

72 David Robinson, *In 3 Years, Chicago Police Have Tripled Their Use of a Secret, Computerized 'Heat List.'*, Medium (May 26, 2016), https://medium.com/equal-future/in-3-years-chicago-police-have-tripled-their-use-of-a-secret-computerized-heat-list-da7a0594ee78.

73 Brianna Posadas, *How Strategic is Chicago's 'Strategic Subjects List'? Upturn Investigates.*, Medium (Jun. 22, 2017), https://medium.com/equal-future/how-strategic-is-chicagos-strategic-subjects-list-upturn-investigates-9e5b4b235a7c ("Our research into the list also found that more than a third of individuals on the list have never been arrested (133,474) and two-thirds of the list have been arrested at least once for any crime (265,210). This contradicts the CPD claim that the list consists of only those with an arrest record. [...] 126,904 individuals on the list have never been arrested or a victim of a crime, and 88,592 of that group have a score greater than 250.")

74 Leila Miller, *LAPD Will End Controversial Program That Aimed To Predict Where Crimes Would Occur*, L.A. Times (Apr. 21, 2020), https://www.latimes.com/california/story/2020-04-21/lapd-ends-predictive-policing-program.

stopped using its predictive program in January 2020.[75] But advocates have noted that LAPD and Chicago are still using predictive policing programs even though they were supposed to shut them down.[76]

Predictive policing tools have come under intense scrutiny for replicating and perpetuating structural racism embedded in the criminal legal system. Data that identifies particular areas as more crime-prone, or particular people as more deserving of suspicion, embeds within it existing prejudices and records that result from disproportionate policing.[77] For instance, higher arrest rates in Black, Latinx, or Native communities do not necessarily reflect higher rates of actual crime; they more likely reflect structural racism in decisions over which communities are more policed and which charges are filed.[78] Data can be skewed by whether people victimized by crime actually file reports, and whether law enforcement actually acts on those reports.[79] Data used for predictive policing may be unreliable for other reasons, too. People who are arrested and charged with crimes may not be responsible for committing those crimes. Even those who are convicted of crimes may not actually be responsible for them for a number of reasons, including the coercive nature of plea agreements, false confessions, and compromised forensic evidence that undergird many convictions. Predictive policing tools that rely on assumptions that past actions actually indicate future propensity to commit a crime are also suspect. These concerns and assumptions exist notwithstanding attitudes about what acts ought to be criminalized or not in the first place.[80]

---

75 Jeremy Gorner & Annie Sweeney, *For Years Chicago Police Rated the Risk of Tens of Thousands Being Caught Up in Violence. That Controversial Effort Has Quietly Been Ended.*, Chi. Trib. (Jan. 24, 2020), https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html.

76 Johana Bhuiyan, *LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws*, The Guardian, Nov. 8, 2021, https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform; Matt Stroud, *Heat Listed*, The Verge, May 24, 2021, https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list.

77 See Ezekiel Edwards, *Predictive Policing Software Is More Accurate at Predicting Policing Than Predicting Crime*, ACLU (Aug. 31, 2016, 12:15 PM), https://www.aclu.org/blog/criminal-law-reform/reforming-police/predictive-policing-software-more-accurate-predicting; Hannah Sassaman, *Covid-19 Proves It's Time to Abolish 'Predictive' Policing Algorithms*, Wired (Aug. 27, 2020), https://www.wired.com/story/covid-19-proves-its-time-to-abolish-predictive-policing-algorithms/.

78 Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need To Be Dismantled.*, MIT Tech. Rev. (Jul. 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

79 Dara Lind, *Why You Shouldn't Take Any Crime Stats Seriously*, Vox (Aug. 24, 2014), https://www.vox.com/2014/8/24/6053035/crime-statistics-reliable-fbi-police-problems.

80 Matthew Hutson, *The Trouble with Crime Statistics*, The New Yorker (Jan. 9, 2020), https://www.newyorker.com/culture/annals-of-inquiry/the-trouble-with-crime-statistics.

Data that identifies particular areas as more crime-prone, or particular people as more deserving of suspicion, embeds within it existing prejudices and records that result from disproportionate policing.

Thankfully, while some jurisdictions continue to use predictive tools,[81] others have determined that such predictive policing tools are biased and thus inappropriate for general use. Some have gone further. In December 2020, Oakland, California became one of the first cities in the country to ban predictive policing and biometric surveillance technologies on recommendations from the city's Privacy Advisory Commission.[82] Similarly, Santa Cruz, California and New Orleans, Louisiana banned predictive policing and facial recognition software[83] and Bellingham, Washington voters passed a ballot initiative banning facial recognition technologies and predictive policing practices.[84]

Predictive policing can also perpetuate existing prejudices in the policing of disabled people - especially disabled people of color. Disability is more prevalent in communities

81 *See generally* David Uberti, *After Backlash, Predictive Policing Adapts to a Changed World*, Wall Street J. (Jul. 8, 2021), https://www.wsj.com/articles/after-backlash-predictive-policing-adapts-to-a-changed-world-11625752931; Jeff Cockrell, *Law and Order and Data*, Chi. Booth Rev. (Mar. 1, 2021), https://www.chicagobooth.edu/review/law-order-data.

82 Brian Hofer, First-In-The-Nation Surveillance Tech Bans, Secure Just. (Jan. 8, 2021), https://secure-justice.org/blog/first-in-the-nation-bans-predictive-analytics-biometric-surveillance-technologies.

83 Ordinance No. 2020-17, City Council of Santa Cruz, https://www.cityofsantacruz.com/home/showdocument?id=80906; New Orleans, Louisiana, M.C.S., Ord. No. 28559, § 1, 12-17-20, https://library.municode.com/la/new_orleans/codes/code_of_ordinances?nodeId=PTIICO_CH147SUTEDAPR; Santa Cruz was the first city to ban predictive policing. Susan Miller, *Santa Cruz Bans Predictive Policing*, GCN (Jul. 1, 2020), https://gcn.com/data-analytics/2020/07/santa-cruz-bans-predictive-policing/315055/; Michael Isaac Stein, *New Orleans City Council Bans Facial Recognition, Predictive Policing and Other Surveillance Tech*, The Lens (Dec. 18, 2020), https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech/.

84 In Bellingham, voters passed the ban as a ballot measure. *VICTORY: Bellingham Voters Ban Facial Recognition, Predictive Policing Software*, ACLU Wash. (Nov. 10, 2021), https://www.aclu-wa.org/news/victory-bellingham-voters-ban-facial-recognition-predictive-policing-software.

of color,[85] and disabled people are also more likely to be lower income,[86] meaning that neighborhoods with higher concentrations of people of color and low-income people, which are historically likely to be subjected to increased policing, will also be neighborhoods with higher concentrations of disabled people. Thus, place-based predictive programs can exacerbate the concentration of policing resources in areas with significant numbers of disabled people. Similarly, person-based predictive programs use a range of data to flag certain people as likely threats, including data that can be related to disability but isn't relevant to whether someone is a threat, raising the risk of profiling as well as self-perpetuating cycles of suspicion and criminalization.

For instance, the Pasco County Sheriff's Office in Florida piloted a "juvenile intelligence analysis" program that created secret lists of students deemed at-risk for potential future crime for reasons including receiving D grades, having 3-4 absences in a quarter, or being victimized by domestic violence - all experiences much more likely to happen to disabled students receiving insufficient support, experiencing chronic illness, or being abused.[87]

These risks, which may not be possible to mitigate or eliminate, can only serve to deepen existing disparities in policing and incarceration that impact disabled people. Consider:

- Developmentally disabled people, including autistic people and people with intellectual disabilities, are at least seven times more likely to encounter police.[88]
- Disabled students, especially Black and Brown disabled students, were among students most frequently subjected to school-related arrests, as documented in the Department of Education's Civil Rights Data Collection for the 2017-2018 school year.[89]

---

85 Martha Ross & Nicole Bateman, *Disability Rates Among Working-Age Adults Are Shaped By Race, Place, and Education*, Brookings Inst.: The Avenue (May 15, 2018), https://www.brookings.edu/blog/the-avenue/2018/05/15/disability-rates-among-working-age-adults-are-shaped-by-race-place-and-education/. This article does not disaggregate Asian communities, however, and may not accurately reflect prevalence of disability in different Asian communities due to poor research methodologies common in research on Asian communities. *See* Rooshey Hasnain, Glenn Ti. Fujiura, John E. Capua, Tuyen Thi Thanh Bui & Safiy Khan (2020), *Disaggregating the Asian "Other": Heterogeneity and Methodological Issues in Research on Asian Americans with Disabilities*, 10 Societies (Special Issue) 58, https://www.mdpi.com/2075-4698/10/3/58/htm#:~:text=According%20to%20the%20American%20Community,lowest%20among%20all%20racial%20categories.

86 Nat'l Council on Disability, National Disability Policy: A Progress Report 76 (2017), https://ncd.gov/sites/default/files/NCD_A%20Progress%20Report_508.pdf.

87 Tim Cushing, *Florida Sheriff's Pre-Crime Software Says D-Students and Victims of Domestic Violence Are Potential Criminals*, TechDirt (Nov. 23, 2020, 11:59 AM), https://www.techdirt.com/2020/11/23/florida-sheriffs-pre-crime-software-says-d-students-victims-domestic-violence-are-potential-criminals/.

88 Dennis Debbaudt & Darla Rothman, *Contact with Individuals with Autism: Effective Resolutions*, 70 FBI L. Enf't Bull. 20 (2001), https://www.ojp.gov/ncjrs/virtual-library/abstracts/contact-individuals-autism-effective-resolutions.

89 Office of Civil Rights, U.S. Dept. of Ed., 2017-18 Civil Rights Data Collection: School-Related Arrests Estimations (2018), https://ocrdata.ed.gov/estimations/2017-2018.

- Disabled people, especially those with cognitive and emotional disabilities, are almost 44 percent more likely to be arrested than nondisabled people.[90]
- Many disabled people experience police brutality because of profiling and misunderstanding characteristics of their disabilities. For instance, autistic people and people with mental illnesses may be perceived as being on drugs, Black people with mobility devices may be profiled as having a violent criminal history,[91] and deaf people may be perceived as noncompliant or defiant for not following verbal orders.[92]

There is no place for discriminatory predictive policing tools in a just society. Reckoning with their past and ongoing harms will require focusing not only on systemic racism but also systemic ableism. Further, the dangers and proven harms of predictive policing tools will only end when governments end use of all discriminatory predictive policing tools - both person-based and place-based. This work will require collaboration with leaders in the movements for racial justice, disability rights, and disability justice. At the same time, policymakers can move away from predictive policing and its role in mass incarceration by diverting funding to non-police resources and social services instead, including non-coercive community-based support and services. Such funding should ultimately prioritize services and programs led by directly impacted people, such as culturally responsive academic and vocational programs as well as peer-led mental health and social work services.

Risk Assessment Algorithms

In recent years, courts and probation and parole offices have turned increasingly to algorithmic risk assessment tools that purport to evaluate whether a person will appear in court or commit another crime, using those evaluations to decide pretrial bail/release and

90 Erin J. McCauley, *The Cumulative Probability of Arrest by Age 28 Years in the United States by Disability Status, Race/Ethnicity, and Gender*, 107 Am. J. Pub. Health 1977 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5678390/.

91 Lateef H. McLeod (2019), Book Review: Black Kripple Delivers Poetry (Leroy Franklin Moore), in 13.1 Wordgathering: A Journal of Disability Poetry and Literature, https://wordgathering.com/past_issues/issue49/reviews/moore.html ("[Leroy] Moore explains that because of the way he walks due to his cerebral palsy the police mistakenly thought that he was drunk and used that a reason to harass them. In Keith Jones's segment of the poem he flows about his encounter with police saying that, 'they be lookin at me tryin to profile the black man talking bout what happen to you damn see there was no gun shot matter of fact I have my own kind of plot I have to run da block shut down because ya trying to hold me down').

92 Abigail Abrams, *Black, Disabled and at Risk: The Overlooked Problem of Police Violence Against Americans with Disabilities*, Time (Jun. 25, 2020), https://time.com/5857438/police-violence-black-disabled/; Leroy F. Moore Jr., Tiny aka Lisa Gray-Garcia & Emmitt H. Thrower, *Black & Blue: Policing Disability & Poverty Beyond Occupy*, in Occupying Disability: Critical Approaches to Community, Justice, and Decolonizing Disability 295 (Pamela Block et al., eds., Springer 2016), http://futuresinitiative.org/criticalracescholarship/wp-content/uploads/sites/228/2019/04/Moore-et-al-Black-and-Blue-Policing-Disability-and-Poverty-Beyond-Occupy.pdf (Leroy Moore and Keith Jones discuss being profiled as drunk, noncompliant, or involved with gang violence due to being Black and disabled).

parole.[93] These algorithms purport to reduce human bias and provide "race-neutral" means to make critical decisions like pretrial release determinations and parole eligibility more fair.

However, evidence shows risk assessment algorithms may actually *perpetuate* bias because they rely on existing demographic and criminal record data, which already reflect intense racial and disability disparities.[94] A 2016 ProPublica investigation found that, in Broward County, Florida, a proprietary risk assessment algorithm used in bail determinations, called COMPAS, was nearly twice as likely to incorrectly assign Black people a high risk of recidivism as white people.[95] At the same time, white people facing charges were more likely overall to be mislabeled as low risk by the algorithm, regardless of other factors. A plaintiff alleged similar concerns in *State v. Loomis* (2016), a case that involved use of the same COMPAS algorithm in Wisconsin, repurposed for sentencing decisions. While the court allowed the algorithm's continued use, the court limited its use, determining that it could not be used to make a decision about a person's incarceration or length of their sentence, and that judges should be warned when algorithms are incorporated into sentencing.[96]

Just as risk assessment scores can perpetuate bias against people of color and low income people, they can also dangerously discriminate against disabled people. The factors used in risk assessment algorithms often serve as strong proxies for experiences of racial and disability marginalization. For instance, risk assessment algorithms have considered the following:

- Level of educational attainment, which may be impacted by disability discrimination and denial of adequate accommodations or services;[97]
- Past arrest or conviction history, which can disproportionately impact disabled people, especially disabled people of color;
- Employment history, which is likely to be spottier for disabled people due to higher rates of unemployment and hiring discrimination;[98]
- Housing stability, which will negatively impact disabled people who have higher

93 Alex Chohlas-Wood, *Understanding Risk Assessment Instruments in Criminal Justice*, Brookings Inst. (Jun. 19, 2020), https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice/.

94 *See generally* Beth Schwartzapfel, *Can Racist Algorithms Be Fixed?*, The Marshall Project (Jul. 1, 2019), https://www.themarshallproject.org/2019/07/01/can-racist-algorithms-be-fixed; Sarah Picard et al., *Beyond the Algorithm: Pretrial Reform, Risk Assessment, and Racial Fairness*, Ctr. for Court Innovation (2019) https://www.courtinnovation.org/publications/beyond-algorithm; Sean Hill, *Bail Reform and the (False) Racial Promise of Algorithmic Risk Assessment*, 68 UCLA Law Review 910 (2021), https://www.uclalawreview.org/bail-reform-and-the-false-racial-promise-of-algorithmic-risk-assessment/.

95 Angwin, *supra* note 62.

96 State v. Loomis, 881 N.W.2d 749, 763-64 (Wis. 2016).

97 Bureau of Lab. Stat., U.S. Dept. of Lab., *People With a Disability Less Likely to Have Completed a Bachelor's Degree* (Jul. 20, 2015), https://www.bls.gov/opub/ted/2015/people-with-a-disability-less-likely-to-have-completed-a-bachelors-degree.htm.

98 Bureau of Lab. Stat., U.S. Dept. of Lab., News Release on Persons with a Disability: Labor Force Characteristics–2021 (Feb. 24, 2021), https://www.bls.gov/news.release/pdf/disabl.pdf.

rates of homelessness and lower income on average;[99] and
- Community and family support, which can negatively impact disabled people who are unpartnered, do not have children, have faced removal of their children from their homes (potentially because of ableist discrimination), lack supportive family members, or are estranged from their families because of abuse.

Risk assessment algorithms create an inherent conflict between accuracy and disability or race neutrality. For instance, criminal history is the most "reliable" predictor of new criminal activity within our current criminal legal system. A person's criminal history is also highly dependent on a variety of factors, ranging from simply what actions have been deemed illegal (regardless of whether they should be) to police and prosecutorial discretion to wrongful convictions. Some groups – especially people with disabilities, people of color, and disabled people of color – face disproportionately higher rates of arrest and incarceration. For these reasons, algorithms incorporating criminal history in every situation to determine an individual person's risk is not necessarily reliable. Beyond questions about accuracy and biased input, however, risk assessment algorithms reinforce the existing criminal legal system itself and its attendant problems. These algorithms examine only whether a person should be considered at risk of committing new crimes, but they do not address the underlying causes of actual violence or biases in law enforcement that disproportionately impact disabled people and people of color.[100]

Use of Criminal Records in Tenant Screening Algorithms and Other Applications

A person's criminal record has ramifications throughout the rest of daily life. Increasingly, tools to screen tenants for apartments, check someone's background for a job,[101] or even check users on a dating site[102] will look at a person's criminal record — and not just their formal record, but other data points that might indicate previous interaction with the criminal

99 U.S. Inter-Agency Council on Homelessness, Homelessness in America: Focus on Chronic Homelessness Among People with Disabilities (2018), https://www.usich.gov/resources/uploads/asset_library/Homelessness-in-America-Focus-on-chronic.pdf.

100 Racial and Ethnic Considerations Workgroup, *Risk Assessments and Racial Disproportionality*, in Washington State Pretrial Reform Task Force, Final Recommendations Report app. B, at 30-33 (2019), https://www.courts.wa.gov/subsite/mjc/docs/PretrialReformTaskForceReport.pdf.

101 *See generally* Marina Duane, Nancy La Vigne, Mathew Lynch, & Emily Reimal, Criminal Background Checks: Impact on Employment and Recidivism, The Urban Institute, Mar. 2017, https://www.urban.org/sites/default/files/publication/88621/criminal-background-checks-impact-on-employment-and-recidivism.pdf.

102 *See, e.g.*, Sara Ashley O'Brien, *Tinder is making criminal background checks available on your dates*, CNN, Mar. 9, 2022, https://www.cnn.com/2022/03/09/tech/tinder-garbo-background-checks/index.html; Keri Blakinger, *Many Dating Apps Ban People Convicted of Felonies. Does That Make Anyone Safer?*, NBC News: Inside Out (May 20, 2021), https://www.nbcnews.com/news/us-news/many-dating-apps-ban-people-convicted-felonies-does-make-anyone-n1267935.

justice system.[103] Criminal records can also adversely impact a person's loan applications and eligibility for critical public benefits like housing subsidies or public housing.

As the use of these tools increases, this approach can end up worsening the already difficult circumstances for returning citizens (formerly incarcerated people). It can also penalize people who have had even a minor brush-up with the law, or who are the victims of data misentry or confusion with another person. Because disabled people are more likely to have police contact and to be incarcerated, exclusionary use of any arrest or criminal records can have a disproportionately negative impact on disabled people, especially disabled people of color.

103 *See generally* Kaveh Wendell, How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times, Consumer Reports (Mar. 11, 2021), https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/.

One recent case shows the devastating consequences of using criminal records in algorithmic decision-making systems. In *Connecticut Fair Housing Center, et al. v. CoreLogic Rental Property Solutions*, Carmen Arroyo sued a tenant screening company after her disabled adult son, Mikhail, was denied permission to join her lease and move in with her.[104]

CoreLogic, one of the leading tenant screening companies, automatically denied their request after generating a report stating that it had found a "criminal court action" relating to Mikhail, but did not provide any other details or information about the record. Ms. Arroyo later learned that the company had referred to records of Mikhail's arrest and citation for a minor shoplifting accusation as a "disqualifying criminal record," even though he was never convicted, the charge was ultimately withdrawn, and Mikhail argued that he did not have the physical capacity to shoplift again. Because Mikhail wasn't allowed to move in with his mother, he was institutionalized for a year.[105] His case is still pending resolution.

104 Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Ctr. for Democracy & Tech. (July 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/.

105 Lauren Kirchner, *Can Algorithms Violate Fair Housing Laws?*, The Markup (Sept. 24, 2020), https://themarkup.org/locked-out/2020/09/24/fair-housing-laws-algorithms-tenant-screenings.

Landlords and property management companies using tenant screening algorithms may violate the law by improperly including criminal history as disqualifying data. Under the Fair Housing Act, landlords can legally consider only an actual conviction, and that conviction's relevance to renting a particular unit to a particular person, in making a housing determination.[106]

Nevertheless, tenant screening algorithms may illegally include arrest records even if there is never a full case, let alone a conviction, and they remove the opportunity for the landlord to consider the applicant's specific circumstances as required. Additionally, use of criminal records as a form of tenant screening can cause and worsen racial and disability disparities in access to housing, too, since people with disabilities and people of color may be more likely to be arrested, charged, and convicted for a variety of offenses.

Tying records of police encounters to tenant screening can also negatively impact survivors of domestic or intimate partner violence, which disproportionately impacts disabled people as well.[107] Although it is illegal to discriminate against victims of domestic violence, when landlords and property managers repeatedly complain that a tenant is a public nuisance due to incidents of violence, this can lead to police contact and potentially eviction.[108]

Similar concerns arise with other tools that conduct background checks based on publicly available data. Many dating apps ban people with felony conviction records, but as with tenant screening algorithms, they do not always contain accurate information about a person's records–and it can be hard for a person to know the reason for their rejection, or to correct errors that have improperly disqualified them. Beyond concerns about accuracy and procedural fairness, the expansion of tools that use a prior felony record as a proxy to disqualify someone from participating in a service perpetuates stigmatization and exclusion of formerly incarcerated people, who are much more likely to have a disability.[109] Such use equates having a criminal record with having a propensity for violence or societal risk without

---

106 Office of Gen. Couns., U.S. Dept. of Hous. & Urb. Dev., Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions (2016), https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.

107 Matthew J. Breiding & Brian S. Armour, The Association Between Disability and Intimate Partner Violence in the United States, 25 Annals of Epidemiology 455 (2015), https://www.sciencedirect.com/science/article/abs/pii/S1047279715001271?via%3Dihub (finding that non-institutionalized disabled women are at greater risk for six types of intimate partner violence and non-institutionalized disabled men are at greater risk for two forms of such violence).

108 *See generally* Gretchen Arnold & Megan Slusser, Silencing Women's Voices: Nuisance Property Laws and Battered Women, 40 A.B.A. L. & Soc. Inquiry 908 (2015), https://nhlp.org/files/001.%20Silencing%20Women%27s%20Voices-%20Nuisance%20Property%20Laws%20and%20Battered%20Women%20-%20G%20Arnold%20and%20M%20Slusser.pdf.

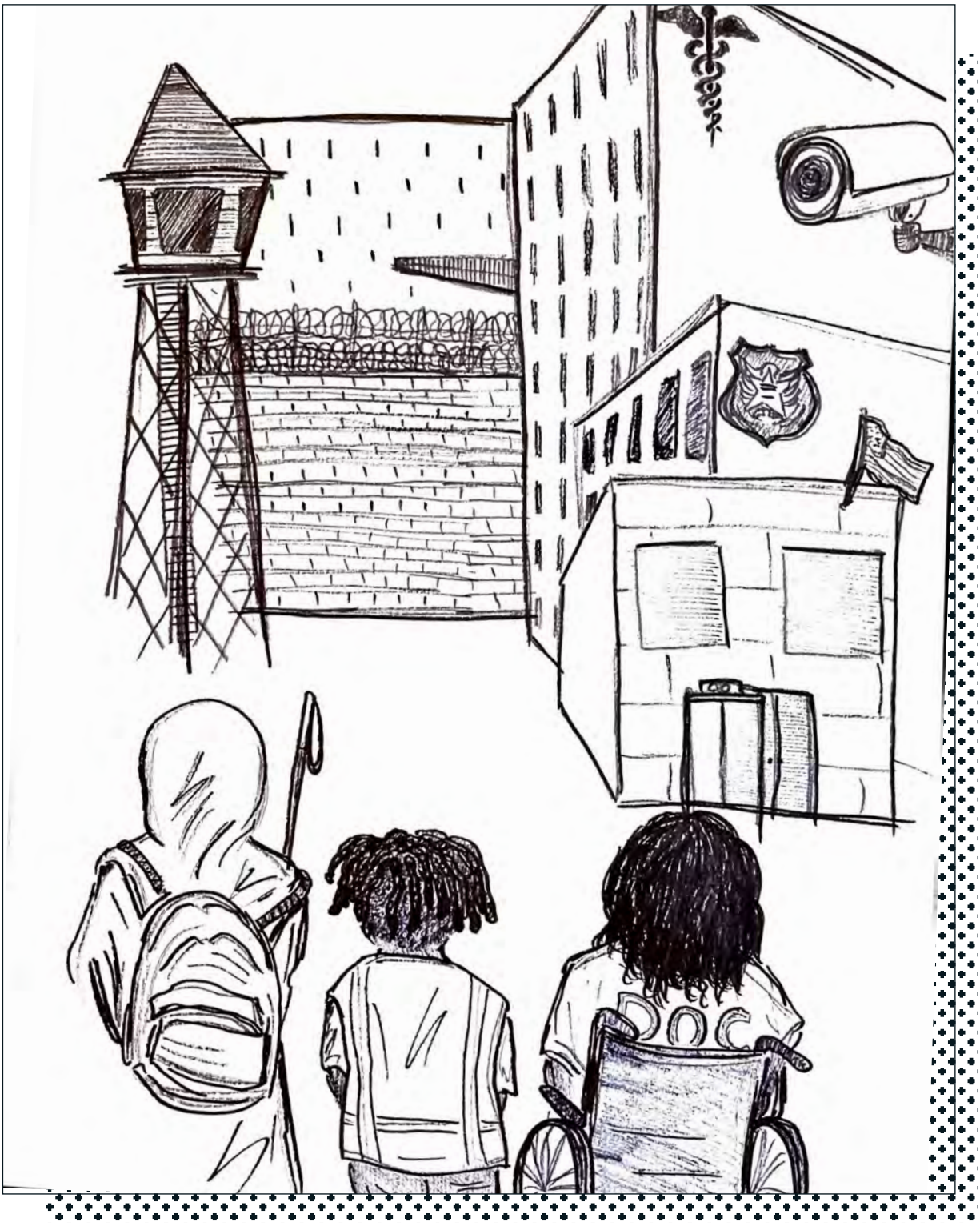
109 See, e.g., Testimony of Talila Lewis to the U.S. Commission on Civil Rights, Briefing: Examining Police Practices and Use of Force (Apr. 20, 2015), at 15-17, https://www.usccr.gov/files/calendar/trnscrpt/Police-Practices-and-Use-of-Force_04-20-2015.pdf. ("People with disabilities also represent the [largest] minority group within our prison and jail system, most studies estimating that some 80 plus percent of our incarcerated population are people with one or more disabilities").

assessing the specific circumstances of that person's past history (or even the possibility of wrongful conviction), and does so after the person has completed their sentence. Such blanket bans disproportionately impact people from marginalized communities, including disabled people, who are subjected to over-surveillance, policing, mass incarceration, and mass criminalization.[110]

Recommendations

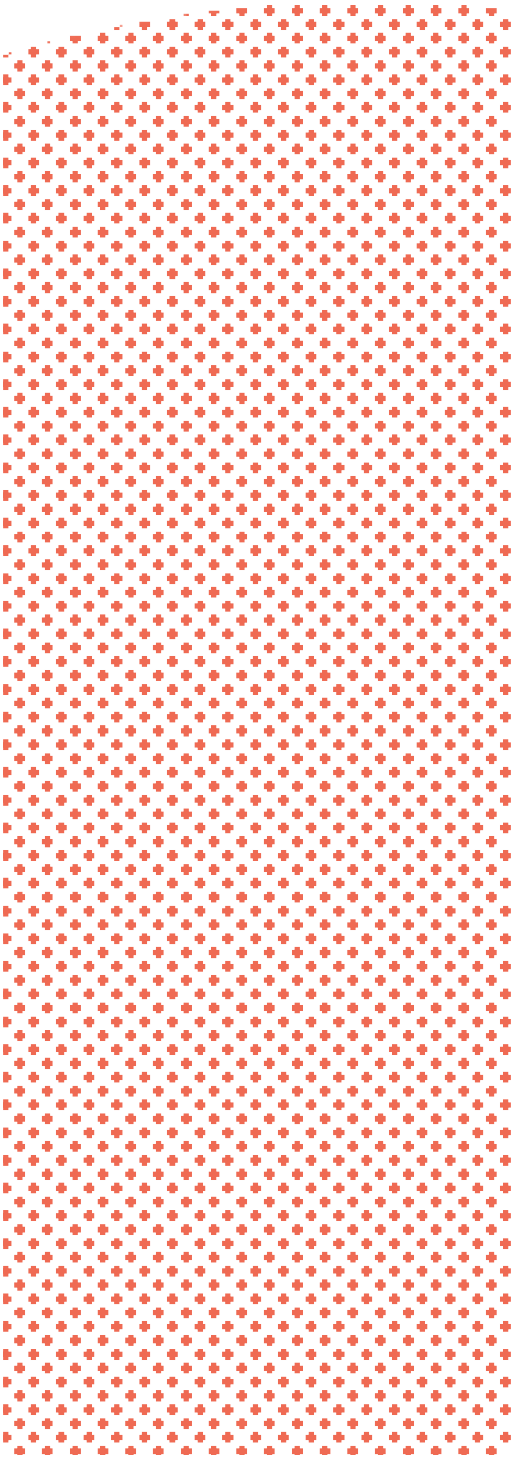
- **Police departments must end use of discriminatory place-based or people-based predictive policing tools.**
- **Courts must ensure that people facing loss of liberty and their legal counsel understand what types of risk assessment tools are being used** by a prosecutor, court, or probation or parole office, and have a meaningful opportunity to raise concerns about and dispute inaccurate or biased information.
- **Employers, landlords, and property management companies must end use of arrest records in screenings for employment or housing.**
- **Employers, landlords, and property management companies should restrict use of eviction, conviction, and other criminal records** to narrow, time-limited purposes requiring evaluation only of directly relevant and recent records, and only at the final stages of employment, housing, or other screenings, as in Fair Chance policies.

110 Blakinger (2021), *supra* note 102.



Illustrated by Lydia X. Z. Brown. Three people together look up at a prison, a hospital, a police station, and a school. The first is a student wearing a hijab and large backpack, with a thin tall cane for orientation. The second is a little person with short dreadlocks wearing a work vest with reflective stripes. The third is a person with dark wavy hair in a manual wheelchair wearing a uniform that says DOC (for Department of Corrections). In front of them, the prison watchtower looms large while a camera watches from the other side. The path to the school is blocked by a metal detector. The hospital and prison have a walkway connecting them.

Health Surveillance



The health industry has similarly taken advantage of automated surveillance technologies. A recent disturbing example of this occurred in January 2022, when Politico broke the news that Crisis Text Line, among the most well-known mental health hotline services, was sharing data from conversations with a company that designs AI programs for customer service.[111] While the data was intended to be anonymized and stripped of personally identifying information, people experiencing extreme states and mental health crises contact hotlines like Crisis Text Line with the expectation of privacy in their most vulnerable moments.[112] Advocates such as Kendra Albert at Harvard's Cyberlaw Clinic noted that, even if it were possible to completely guarantee anonymity in data taken from long, detailed conversations such as those captured by the Crisis Text Line, the mere fact that a for-profit AI developer was using data from conversations about people's experience of intense suicidality and other extreme states directly contravenes the purpose of confidential peer support and crisis counseling. After facing criticism from mental health and privacy advocates, Crisis Text Line ended its data-sharing partnership less than a week after Politico broke the news.[113]

Disabled advocates have long resisted the idea that disability should always be understood solely or primarily as a health or medical issue. Nonetheless, disabled people's

111 Alexandra S. Levine, *Suicide hotline shares data with for-profit spinoff, raising ethical questions*, Politico (Jan. 28, 2022), https://www.politico.com/news/2022/01/28/suicide-hotline-silicon-valley-privacy-debates-00002617.

112 *See, e.g.*, Twitter Posts of Kendra Albert, on Jan. 30, 2022, https://twitter.com/KendraSerra/status/1487914046066237442.

113 John Hendel, *Crisis Text Line ends data-sharing relationship with for-profit spinoff*, Politico (Jan. 31, 2022), https://www.politico.com/news/2022/01/31/crisis-text-line-ends-data-sharing-00004001.

lives and experiences are often framed and thought of as private medical problems or public health issues. As a result, health-related data and surveillance are of particular importance for disabled people, who are more likely to encounter health-related service settings, use health-related products or programs, and to live in/with bodies and minds categorized as health issues.

Invasive, coercive, and opaque data collection practices can leave people with disabilities without acceptable options when they seek to exercise their rights. Far too frequently, disabled people are confronted with no-win situations regarding how data about their care and health will be collected, processed, shared, and retained. All too often, in order to access benefits, use an app, connected device, or even secure medical treatments, many people must consent to using technology and the data practices associated with it, without having a complete, meaningful opportunity to weigh alternative options and make informed choices about how they want data about their health to be handled. The only other alternative may be to seek out a different provider, which can be difficult if not impossible for many disabled people who struggle to find doctors who are respectful, knowledgeable, have accessible offices, or accept their insurance (especially for disabled people on Medicaid).

In a recent report published by the International Digital Accountability Council (IDAC), researchers revealed that of 152 Android health apps related to pregnancy, babies, menstruation, mental health, fitness, and weight loss:[114]

- **125 apps (82%) disclosed that they collect personal information but only 66 (54%) disclosed that they collect health information;[115]**
- **21 of the fitness and weight loss apps, 14 of the pregnancy and menstruation related apps, and six of the mental health apps requested access to people's precise location;[116]**
- **Two apps exposed people's sensitive health information and personally identifying information including emails and phone numbers through unencrypted transmissions;[117] and**
- **Two apps didn't provide a privacy policy at all.[118]**

IDAC's team wrote, "[w]hen it comes to sharing our most health sensitive data, our laws place a strong emphasis on the notion of notice and consent. But notice often means that apps carefully include a vague and legalistic statement about data collection and sharing; and consent often means that a person clicks through a jargon-filled document without reading or understanding the disclosures that are being made."[119]

114 Holden Williams, Ginny Kozemczak & Dan Kinney, *Digital Health is Public Health: Consumers' Privacy & Security in the Mobile Health App Ecosystem*, International Digital Accountability Council (Dec. 15, 2021), https://digitalwatchdog.org/wp-content/uploads/2021/12/IDAC-Health-Report-For-Publication-1.pdf.

115 *Id.* at 7.

116 *Id.* at 8.

117 *Id.* at 4.

118 *Id.* at 5.

119 *Id.* at 1.

Furthermore, people with disabilities may not be able to individually use certain services and products if they are not accessible. For instance, if tech-assisted systems are not designed to be accessible, people who rely on those systems will not be able to independently access or share their health data without the help of another person. That design flaw can directly lead to privacy harms because disabled people are forced to either forgo the service/ treatment or seek help and reveal personal health information.

Disabled people face a number of issues related to health data and automated use of such data. Below, we discuss medications and medical devices that track compliance, use of predictive analytics to detect or predict likelihood of mental illness and other disabilities, and electronic visit verification technology adoption.

Medications and Medical Devices That Track Compliance

Increasingly, automated tracking technology has been used to track medications and medical compliance. In theory, tracking compliance could help doctors determine compliance with medical regimens. However, automating surveillance does not necessarily promote better health outcomes, and in fact may instead deter people experiencing medical problems from seeking any treatment.

In 2017, the FDA approved Abilify MyCite, an antipsychotic medication that contains a sensor in each pill tracking whether or not a person has taken their medication - marking the first time the agency approved any drug with a "digital ingestion tracking system."[120] The justification for its development and use lies primarily with the assumption that people with psychosocial disabilities may be inconsistent in following medication directions, and therefore will not gain the full benefit of following a prescribed medication regimen without monitoring and assistance.[121] Yet people with psychosocial disabilities, much like nondisabled people, may wish to make their own decisions about whether to follow a doctor's instructions at their own risk, or may have sought a second opinion that differed with the original doctor. Either way, people may not wish that their medical habits be surveilled in such an intrusive way.

Similarly invasive technologies exist in some medical devices designed to assist with other disabilities and chronic illnesses. Continuous glucose monitoring (CGM) systems monitor glucose levels in a person's body for people with diabetes. Continuous positive airway pressure (CPAP) machines help patients track their sleep and breathing for obstructive sleep apnea. These systems can be either "semi-invasive" and rely on an external sensor attached to the person's body, or can consist of an implant placed beneath the skin.[122] Some

120 Press Release, U.S. Food & Drug Admin., FDA Approves Pill With Sensor That Digitally Tracks If Patients Have Ingested Their Medication (Nov. 13, 2017), https://www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication.

121 Shain Neumeier, *New Compliance Tracking Drugs Violate Human Rights*, NOS Magazine (Dec. 18, 2017), http://nosmag.org/compliance-tracking-drugs-violate-human-rights-abilify-mycite/.

122 Frost & Sullivan, *Automated Blood Glucose Monitoring*, Alliance of Advanced BioMedical Engineering (2018), https://aabme.asme.org/posts/automated-blood-glucose-monitoring.

companies that manufacture these systems advocate for, and rely on, use of digital remote monitoring to maintain compliance and predict likelihood of medication follow-through.[123]

While there may be some positive uses of these systems, they still pose significant privacy and surveillance concerns.[124] Patients, particularly those with disabilities, may want more autonomy and control over their lives and not to be under their doctor's microscope, even while still wanting to receive treatment. Even if the approach is framed as "optional," the power dynamics of a physician-patient or insurer-insured relationship may lock patients into certain treatments even if it subjects them to constant surveillance. Disabled people are more likely to need medical devices or treatments, and less likely to have meaningful access to a range of respectful providers and accessible treatment options.

Patients may also worry about the implications of other entities having access to the data because it could be used to make or influence health care decisions, predict outcomes, or modify or deny services to disabled people potentially in a discriminatory way. An insurance company may be able to access such compliance data and make decisions about coverage or premiums based on it.[125] In 2019, news coverage revealed that a pregnancy app was sharing information about people's struggles with fertility directly with employers, in a de-identified, aggregated manner that nevertheless gave employers extraordinary access to profoundly sensitive information about their employees.[126]

Use of Predictive Analytics to Detect or Predict Likelihood of Mental Illness and Other Disabilities

A person's sensitive health information, such as whether the person has mental health issues or is suicidal, may be inferred from their online actions. In one experiment, researchers developed an AI program that could accurately predict people's future, confirmed diagnoses of mental illnesses based on an analysis of their Facebook posts and private messages in

123 *See e.g.*, John Hopefl, *Supporting Remote Patient Monitoring (RPM) By Leveraging Machine Learning To Predict Dropout Risk*, Glooko (Aug. 12, 2020), https://glooko.com/supporting-remote-patient-monitoring-rpm-leveraging-machine-learning-predict-dropout-risk/.

124 Deven McGraw & Kenneth D. Mandl, *Privacy Protections to Encourage Use of Health-Relevant Digital Data In a Learning Health System*, 4 Nature Partner J. Digital Med. (2021), https://www.nature.com/articles/s41746-020-00362-8 (noting that HIPAA protections do not apply outside of health-oriented organizations/companies, and thus do not sufficiently protect all health-related data, particularly "data [that is] sensitive because of stigma, health, and financial implications associated with having limited resources").

125 Marshall Allen, *You Snooze, You Lose: Insurers Make the Old Adage Literally True*, ProPublica (Nov. 21, 2018), https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true (describing insurance company accessing CPAP data to determine whether to cover the cost).

126 Drew Harwell, *Is your pregnancy app sharing your intimate data with your boss?*, Washington Post (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

the prior year.[127] In another experiment, researchers created a computational model that could accurately predict Twitter users' future diagnoses of mental illnesses.[128] In this model, researchers were able to successfully predict diagnoses of depression and post-traumatic stress disorder based on content analysis of the "affect, linguistic style, and context" from people's tweets for several months leading up to their initial diagnoses, and were able to do so even with content posted months before the person's first depression diagnosis.[129]

Big Tech companies themselves are trying to get into the game as well. They collect extensive amounts of data for internal research. Facebook already uses its content analysis AI to scan nearly every person's posts for signs of possible suicidality – and shares that data with emergency responders – without obtaining affirmative consent.[130] As recently as September 2021, Apple researchers announced a partnership with UCLA and Biogen researchers to explore potential for iPhone "sensor data that includes mobility, physical activity, sleep patterns, typing behavior" and facial expressions to develop algorithms to detect depression, aging-related cognitive disabilities, and other targeted disabilities.[131] Within the disabled advocacy community, many people experiencing chronic or acute suicidality beg their Facebook friends not to report their posts seeking support or help, because of Facebook's habit of deactivating or severely limiting account features for people whose posts are flagged as potentially indicative of suicidality both by manual reports and by algorithm.[132]

The expansion of existing automated content moderation tools in the near future poses further concerns about disabled people's ability to use social media as a tool to connect, organize, and find support around distressing experiences.[133] People experiencing suicidality

---

127 Grace Huckins, *An AI Used Facebook Data to Predict Mental Illness*, Wired (Dec. 14, 2020) https://www.wired.com/story/an-ai-used-facebook-data-to-predict-mental-illness/.

128 Andrew G. Reece et al., *Forecasting the Onset and Course of Mental Illness With Twitter Data*, 7 Sci. Rep. (2017), https://www.nature.com/articles/s41598-017-12961-9.

129 *Id.*

130 Benjamin Goggin, *Inside Facebook's Suicide Algorithm: Here's How the Company Uses Artificial Intelligence to Predict Your Mental State From Your Posts*, Bus. Insider (Jan. 6, 2019), https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12.

131 Rolfe Winkler, *Apple is Working on iPhone Features to Help Detect Depression, Cognitive Decline*, Wall Street J. (Sept. 21, 2021), https://www.wsj.com/articles/apple-wants-iphones-to-help-detect-depression-cognitive-decline-sources-say-11632216601.

132 Jordan Novet, *Facebook is using A.I. to help predict when users may be suicidal*, CNBC (Feb. 21, 2018), https://www.cnbc.com/2018/02/21/how-facebook-uses-ai-for-suicide-prevention.html; Benjamin Goggin, *Inside Facebook's suicide algorithm: Here's how the company uses artificial intelligence to predict your mental state from your posts*, Business Insider (Jan. 6, 2019), https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12.

133 Disparities in Suicide, Centers for Disease Control https://www.cdc.gov/suicide/facts/disparities-in-suicide.html; Aneri Pattani, *Pandemic Unveils Growing Suicide Crisis For Communities Of Color*, KHN Science Friday (Aug. 20, 2021), https://www.sciencefriday.com/segments/suicide-crisis-communities-of-color/.

may have other underlying disabilities, and chronic and acute suicidality are in themselves experiences of psychosocial disability or neurodivergence. Particularly as people from other marginalized communities are more likely to experience suicidality, automated analysis and monitoring for suicidality can have a chilling effect on people's ability to seek support for distressing experiences. Moreover, advocates must be vigilant about additional applications of machine learning programs that may predict diagnoses of mental illnesses – such as use in employment background checks, tenant screening, dating websites, or any of a myriad of other applications.

Electronic Visit Verification Technology Adoption

Electronic Visit Verification (EVV) technology is another form of tech-assisted surveillance that directly impacts people with disabilities. EVV is used to track various aspects of home care and personal care attendants such as hours worked and the location where the services were provided. In practice, EVV programs require people with disabilities and care workers alike to record the exact hours worked, exact tasks performed, and exact locations where services were provided, in an attempt to combat fraud and increase efficiency.

EVV use is required in certain circumstances. Federal law requires states to adopt and deploy EVV for Medicaid recipients receiving personal care attendant services by January 2021 (a delayed implementation deadline), and will require the same process for people receiving Home and Community Based Services funding beginning in 2023.[134] State agencies also use EVV monitoring.[135] EVV systems can be deployed through specific devices in the home, mobile apps, or websites that log real-time hours and location information.[136]

134 Centers for Medicare & Medicaid Services, Department of Health & Human Services, Electronic Visit Verification (EVV) https://www.medicaid.gov/medicaid/home-community-based-services/guidance/electronic-visit-verification-evv/index.html ("Section 12006(a) of the 21st Century Cures Act mandates that states implement EVV for all Medicaid personal care services (PCS) and home health services (HHCS) that require an in-home visit by a provider."). States that do not use EVV receive reduced Medicaid funding.

135 s.e. smith, *Electronic Visit Verification: A Threat to Independence for Disabled People*, Rooted in Rights (July 31, 2018), https://rootedinrights.org/electronic-visit-verification-a-threat-to-independence-for-disabled-people/.

136 *Id.*

***

Wiley Reading, a white trans man with ADHD, currently provides personal care attendant services to a woman with cerebral palsy.

"The past seven years I've worked for a woman with cerebral palsy and I am paid through [a fiscal services intermediary]. They recently started requiring EVV, which makes doing my timesheets an absolute nightmare. Because of the limitations of the EVV system, we can't record time if more than one carer needs to be present (like for a doctor's appointment where she needs to use a hoyer lift [to transfer in or out of a wheelchair], or when one of us is training a new carer), or if we need to run errands for her outside of her home. Also, if we mess up our timesheets and don't realize the error/fix them within a small window of time, we are not given back pay. EVV also routinely generates incorrect timesheets even without user error, resulting in lost wages for me."

For many disabled people, EVV requirements are a significant threat to their autonomy.[137] For example, EVV technologies require beneficiaries to log and approve hours worked. This can be difficult for individuals who may have to log and classify multiple interactions every single day.[138] Accurately logging multiple services that may occur during one visit, like assisting with toileting, household cleaning, and assistance with medication, may all need to be logged independently and accurately each time they occur – creating, in the name of fraud detection, a highly revealing and detailed chronicle of a person's most intimate needs in their daily life, and at the same time taking time away from actually providing care.[139]

EVV can also expose people with disabilities to increased location, video, and sound surveillance. Some EVV systems use GPS tracking, cameras, and microphones in an effort to log and track home care services, especially as workers may be geofenced to limited locations or required to start and end service provision in disabled people's homes without any flexibility.[140] The Centers for Medicare & Medicaid Services (CMS) have issued guidance indicating that GPS tracking is unnecessary, but they have also indicated that states are allowed to use it.[141]

Additional CMS guidance in 2019 undermined advocates' attempts to create less invasive systems by explicitly stating that web-based timesheets modeled on the old paper timesheets were non-compliant because they were not sufficiently detailed.[142] These persistent and passive types of tracking and monitoring systems subject disabled people to unnecessary surveillance and control for simply receiving home-based services.[143] The current system sets up an impossible choice: either live at home and be subjected to intrusive EVV surveillance technologies or receive services in institutional settings. Like

137 *Id.*

138 *Id.*

139 *Id.*

140 *Id.*

141 Frequently Asked Questions: Section 12006 of the 21st Century Cures Act: Electronic Visit Verification (EVV) Systems for Personal Care Services (PCS) and Home Health Care Services (HHCS), Centers for Medicare and Medicaid Services, https://www.medicaid.gov/federal-policy-guidance/downloads/faq051618.pdf; Centers for Medicare & Medicaid Services Electronic Visit Verification (EVV) Stakeholder Open Door Forum (Nov. 7, 2018), at 9 https://dhhr.wv.gov/bms/Programs/WaiverPrograms/EVV/Documents/20181107_CMS_Stakeholder_Transcript.pdf (Ralph Lollar stated, "we need to be clear about the fact that we cannot prohibit states from using GPS").

142 Centers for Medicare and Medicaid Services, Additional EVV Guidance, CMCS Informational Bulletin (Aug. 8, 2019), https://www.medicaid.gov/federal-policy-guidance/downloads/cib080819-2.pdf; Alexandra Mateescu, Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care, Data & Society (Nov. 2021), at 14, https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf.

143 Disability Rights Education & Defense Fund, *DREDF Opposes Electronic Visit Verification (EVV) When It Threatens Disabled People's Civil and Privacy Rights and Impedes Personal Choice, Autonomy, and Community Participation* (Mar. 7, 2018), https://dredf.org/2018/03/07/dredf-statement-on-electronic-visit-verification/.

other algorithmic systems deployed in the public benefits context, "EVV has contributed to the growing landscape of punitive technologies that target and criminalize both low-wage workers and public benefits recipients."[144]

Recommendations:

- **Data that is used for diagnosis, assessment, and ongoing treatment of medical conditions (such as data collected by GCM or CPAP devices, or health-related apps) should not be used by insurers or other entities** to discriminate against people with disabilities and chronic illnesses.
- **Developers and medical professionals should limit data collection and sharing to only the minimum necessary for a specific task.** Even so, developers and medical professionals should ensure that patients have a meaningful ability to opt-out of data sharing as well as limit or change data sharing settings in health-related software, apps, or devices.
- **Researchers and developers should obtain meaningful consent from people using social media platforms before using or retaining their data to develop AI/ML models that can predict or identify mental illnesses or other disabilities.** This includes ensuring that people receive regular, meaningful reminders about use of their data, and their ability to change their mind and opt-out of such research and use, including deleting their data.
- **States should clarify that compliance with federal EVV requirements does not require precise GPS location data**, and act to protect workers and people receiving care from forced disclosure of that data.

144 Mateescu (2021), *supra* note 142, at 3.

Surveillance at Work

Employers have adopted surveillance technologies to monitor, assess, discipline, and modify behavior of workers, both for purposes directly related to job performance and for purposes unrelated to job performance. Two applications of surveillance technologies at work are programs used to monitor workers on the job, and programs used to encourage or enforce company wellness programs. Both of these can disproportionately harm disabled workers, who are more likely to face adverse actions in reaction to their disabilities, more susceptible to new and exacerbated injuries and illnesses in the workplace, and less able to comply with arbitrary standards for health and wellness because of their disabilities.

Algorithmic management and surveillance

Companies use algorithmic decision-making systems extensively in hiring, and those systems can discriminate against disabled people applying for jobs.[145] But algorithmic decision-making does not stop at recruitment. Automated programs can include computer software that uses a webcam or screen monitoring to capture live images or video feeds of a worker, their environment, and their activities. They can also include technologies that monitor performance and productivity to increase efficiency for the employer, while reducing or eliminating workers' ability to take breaks, rest between tasks, or move at a comfortable physical pace. Workers who take bathroom breaks while working from home, or pause to rest too much while working

145 *See* Lydia X. Z. Brown, Ridhi Shetty & Michelle Richardson, *Algorithm-driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?*, Ctr. for Democracy & Tech. (2020) https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination/.

in a warehouse, can be subjected to automated discipline including docked pay for time not working, denial of promotions and raises for inefficiency, and sometimes even termination by algorithm.[146]

An increasing number of employers across sectors have adopted intrusive software, using an array of sensors on workers' phones, computers, and other workplace settings to monitor their workers, evaluate their performance, make disciplinary decisions, and enforce expectations for their work.[147] Employers use automated monitoring and assessment and evaluation software in a variety of work contexts - across industries and types of workplaces, including on-site work, work requiring travel away from a central site (such as delivery work), and remote work. This software affects workers in all types of jobs, including delivery, warehouses, gig work, office work, teaching, retail, and more.

146 Colin Lecher, *How Amazon automatically tracks and fires warehouse workers for 'productivity'*, The Verge (Apr. 25, 2019), https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

147 Matt Scherer, Warning: Bossware May Be Hazardous to Your Health, Ctr. for Democracy & Tech. at 8 (2021), https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/ ("[E]mployers today can track workers' activities continuously and with a previously unattainable level of detail. [...] These advances in worker tracking have been accompanied by equally transformative advances in algorithmic management. Companies can feed the data collected by worker surveillance and monitoring systems into algorithms that assign, optimize, and evaluate workers.")

***

Alma (not their real name) is a sick, disabled, neurodivergent Asian American gender queer academic with multiple disabilities. They shared this story:

"My previous employer always said they do not hover over their employees' shoulders and they do not micromanage their employees. I came to find out this was not the case: my supervisor was spying on my Outlook calendar schedule and online activity as an administrator who can view all that I can do. I am a sick, disabled, and neurodivergent person. I require breaks in between meetings. When she found out I was taking breaks, she began to micromanage my schedule, my tasks, my time. She also had access as an admin of our advising software that keeps track of advisor-student meetings. I know a lot of advisors who are being policed through this software: how many students we meet with, what we discuss, whether our notes are thorough enough, are we making enough referrals.

"They look at the number of students you are meeting with as a measure of success instead of the quality of interactions. I pushed back and developed qualitative surveys which show even though I had fewer meetings with students, each meeting was quality where I took the time to learn from them, listen, and how can I support them."

Automating worker and workflow management, discipline, promotions, and terminations can cause and exacerbate disabilities as well as constitute disability discrimination.[148] Enforcing faster pace of work and higher pressure on the job can push workers to dangerous extremes and potentially put them at risk for physical injury, either in a single accident or by causing repetitive motion injuries.[149] That pressure can also cause higher rates of mental health distress, termed "job strain" by industrial and organizational psychologists,[150] that itself can constitute a disability as it causes and exacerbates anxiety, depression, cognitive disability, and trauma responses.[151] Further, algorithmically enforced workplace policies can punish workers who need additional cognitive processing time or have pressing bathroom needs due to a range of possible disabilities and chronic illnesses.

Such policies and practices disproportionately harm disabled workers, who often require opportunities for rest, flexibility, and supportive work environments to attend to disability-related needs. Disabled people – regardless of race or gender – are more than twice as likely to be unemployed in the United States as non-disabled people, according to the Bureau of Labor Statistics.[152] Disabled workers who work in low-wage and precarious jobs without other financial support are particularly vulnerable to exploitative and dangerous practices because of the need to keep a job, no matter how unsafe or unjust the working conditions. Disabled people of color who face the lifelong impacts of both ableism and racism are also more likely to face systematic employment and hiring discrimination, and believe they have less bargaining power to ask and advocate for better working conditions.[153]

Additionally, these programs may be in violation of the law (both general labor laws and disability rights law), despite inconsistent avenues for enforcement. Employers who adopt bossware systems,[154] particularly those that are used to assess employee performance or

148 *Id.* at 24-27.

149 *Id.* at 14.

150 Ehsanollah Habibi, Siamak Poorabdian & Mahnaz Shakerian, Job Strain (Demands and Control Model) as a Predictor of Cardiovascular Risk Factors Among Petrochemical Personnel, 4 J. Ed. & Health Promotion 1 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4389361/.

151 Samuel B. Harvey et al., *The Role of Job Strain in Understanding Midlife Common Mental Disorder: A National Birth Cohort Study*, 5 Lancet Psychiatry 498 (2018), https://www.thelancet.com/journals/lanpsy/article/PIIS2215-0366(18)30137-8/fulltext.

152 America's Recovery: Labor Market Characteristics Of People With A Disability, U.S. Bureau of Lab. Stat. (Oct. 2021), https://www.bls.gov/spotlight/2021/labor-market-characteristics-of-people-with-a-disability/pdf/labor-market-characteristics-of-people-with-a-disability.pdf.

153 Nanette Goodman, Michael Morris & Kelvin Boston, Financial Inequality: Disability, Race, and Poverty in America, National Disability Institute (Feb. 2019) at 13-14, https://www.nationaldisabilityinstitute.org/wp-content/uploads/2019/02/disability-race-poverty-in-america.pdf; Rob Gould, Courtney Mullin, & Sarah Parker Harris, Race, Disability, and Employment: An ADA Knowledge Translation Center Research Brief, University of Illinois at Chicago Department of Disability and Human Development (2021), https://adata.org/sites/adata.org/files/files/Race_Disability_and_Employment_FINAL_LP.pdf.

154 "Bossware" refers to technologies that allow for the continuous surveillance of workers' activities and/or automation of the task of supervising them. Scherer, *supra* note 147, at 4.

perform managerial functions, will violate the Americans with Disabilities Act if they use them to target or unfairly disadvantage disabled workers, or if they deploy such systems without providing disabled workers an opportunity to request accommodation.

Non-disabled workers also enjoy some protection as well under the Occupational Safety and Health Act (OSH) Act. The OSH Act established a research unit within the CDC called the National Institute for Occupational Safety and Health (NIOSH) to identify and study threats to workers' health, as well as a federal agency (the Occupational Safety and Health Administration, or OSHA) to issue and enforce regulations protecting worker safety. The OSH Act both requires employers to comply with OSHA regulations and also imposes a general duty on employers to protect workers from "recognized hazards" to their health and safety. Although no published NIOSH studies examine the effects of bossware specifically, numerous NIOSH studies have demonstrated the dangers of job strain,[155] repetitive motion injuries,[156] and fatigue,[157] making those threats well-recognized and (at least arguably) subject to employers' general obligation to protect workers' well-being under the OSH Act.

Nonetheless, OSHA has not issued standards specifically protecting workers from these harms, either as a general matter or in the context of automated surveillance and management systems. Additionally, the OSH Act doesn't give individual workers the right to sue employers for health and safety violations, and OSHA's enforcement authority is quite limited compared to other agencies, such as the EEOC and DOL, that enforce laws protecting workers.

Monitoring workers' health via employer-sponsored health and wellness programs

While employers may be turning to algorithm-driven decision making to enforce a dangerous pace of work and to surveil workers to the detriment of their mental health, some are (ironically) implementing health and wellness programs for the supposed benefit of those employees. These programs, which are typically voluntary, can provide benefits and pay incentives for participating workers who achieve weight, heart health, walking, smoking cessation, or dietary goals, all of which may be assessed with biometric data or tracked in an app and shared with an employer.[158] Additionally, employers may offer not only positive

155 *See generally* Nat'l Inst. for Occupational Safety & Health, Dept. of Health & Hum. Serv., Stress at Work (2013), https://www.cdc.gov/niosh/topics/stress/default.html.

156 *See generally* Nat'l Inst. for Occupational Safety & Health, Dept. of Health & Hum. Serv., Ergonomics and Musculoskeletal Disorders (2018), https://www.cdc.gov/niosh/topics/ergonomics/default.html.

157 *See generally* Nat'l Inst. for Occupational Safety & Health, Dept. of Health & Hum. Serv., Work and Fatigue (2021), https://www.cdc.gov/niosh/topics/fatigue/default.html.

158 Nancy Sansom, *New Apps Improve Employee Wellness*, Corp. Wellness Mag. (last updated 2022), https://www.corporatewellnessmagazine.com/article/new-apps-improve-employee-wellness; Joanne Sammer, *Employer Incentives Encourage Employees to Quit Smoking*, SHRM (Oct. 29, 2018) https://www.shrm.org/hr-today/news/hr-magazine/1118/pages/employer-incentives-encourage-employees-to-quit-smoking.aspx.

incentives to encourage participation in their programs, but may also impose sanctions for employees who decline to participate, such as additional insurance surcharges.[159]

Health programs can inherently discriminate against disabled workers, whose disabilities and chronic illnesses may make it impossible to achieve a "healthy" standard as judged by expectations for nondisabled people who are also thin and conventionally attractive, even though fatness and disability do not necessarily mean a person is unhealthy or unwell.[160] In 2016, the EEOC issued a final rule on workplace wellness programs and Title I of the Americans with Disabilities Act, stipulating that such programs cannot ask for or require disability-specific information, and that incentives for health-contingent programs must be equally available to disabled and nondisabled workers alike.[161] In practice, however, incentivizing workers to lower blood pressure, walk a certain number of paces in a day, lose weight, or reduce cholesterol places undue pressure on disabled workers to either opt out and not receive any incentives, or to participate knowing that they may be unable to attain the program's stated goals.

Additionally, data collected by wellness programs could easily be accessed by third parties if not protected sufficiently.[162] Third party sharing can further jeopardize disabled people's privacy and increase risk of discrimination. Such information may not be protected by HIPAA if it is not held with a health care provider, though some wellness programs are provided as part of an employer-sponsored group health plan.[163] City employees in Houston, Texas, for instance, were required to share information about "their disease history, drug and seat belt use, blood pressure and other delicate information" with an online wellness company whose authorization form disclosed that the company might share information with third-party vendors or even in places "reviewable to the public."[164] Disabled people already face frequent

---

159 Jay Hancock & Kaiser Health News, *Workplace Wellness Programs Put Employee Privacy At Risk*, CNN (Oct. 2, 2015), https://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/index.html.

160 Camila Strassle, *How Workplace Wellness Programs Harm People with Disabilities*, Justice Everywhere (Sept. 17, 2018), http://justice-everywhere.org/health/how-workplace-wellness-programs-harm-people-with-disabilities/.

161 29 C.F.R. §1630.14; U.S. Equal Emp. Opportunity Comm'n, Final Rule on Employer Wellness Programs and Title I of the Americans with Disabilities Act (2016), https://www.eeoc.gov/regulations/eeocs-final-rule-employer-wellness-programs-and-title-i-americans-disabilities-act.

162 *See, e.g.*, Drew Harwell, *Is your pregnancy app sharing your intimate data with your boss?*, Washington Post (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

163 Dinah Wisenberg Brin, *Wellness Programs Raise Privacy Concerns over Health Data*, SHRM (Apr. 6, 2016), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/wellness-programs-raise-privacy-concerns-over-health-data.aspx; U.S. Department of Health & Human Services, HIPAA Privacy and Security and Workplace Wellness Programs https://www.hhs.gov/hipaa/for-professionals/privacy/workplace-wellness/index.html.

164 Hancock, *supra* note 159.

invasions of privacy and risk of heightened discrimination because of their disability status; making health-related data potentially available to unregulated, uncontrolled third-parties or the public is dangerously invasive.

Recommendations

- **The EEOC, Department of Labor, and other regulators should issue clearer guidance** on how health-related apps and software used in employer-sponsored wellness programs - as well as employer policies and incentives attached to such programs - must comply with nondiscrimination laws, including disability rights laws. Such guidance should also ensure that employee participation in these programs remains meaningfully voluntary, and does not potentially single out disabled people for declining to participate.
- **NIOSH should conduct additional research on the effects of bossware on workers' mental and physical health.**
- **OSHA should adopt specific standards requiring employers to eliminate the harmful effects of bossware.**

Conclusion

Disabled people face heightened risks and danger from surveillance tools and algorithm-driven systems in a range of contexts. While these tools are often aimed at preventing bad outcomes (such as academic dishonesty and threats of violence) or are nominally aimed at incentivizing positive outcomes (such as improved health and efficiency at work), disabled people are often at a severe disadvantage when surveillance is used to make decisions about them. This report discussed a wide variety of instances where disabled people were discriminated against, had their lives made more difficult, or were otherwise harmed because a poorly-trained algorithm or artificial intelligence system did not incorporate the needs of disabled people.

Fortunately, there are ways to help prevent this from happening. Our recommendations and cited materials provide a starting point for policymakers, companies and advocates. Effective policy change must address the overarching objectives of algorithmic surveillance tools, and by addressing underlying harmful policies, obviate the need for use of dangerous algorithmic surveillance tools. Regulatory intervention must take into account suspect promises that technological programs can self-audit for bias and discrimination, or that simply equalizing outcomes will sufficiently address harmful impacts of algorithmic surveillance tools. Many of these tools' actual purposes are themselves questionable at best, and unjust at worst. And effective regulation will not only limit what data schools, employers, police, courts, and private software companies can collect in their respective contexts, but how they can use it, how long it will be retained, who can access it, and what its overall purpose may be for. Only then can we make progress in addressing this problem.

cdt.org

cdt.org/contact

Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

202-637-9800

@CenDemTech

CENTER FOR
DEMOCRACY
& TECHNOLOGY