

Ableism And Disability Discrimination In Surveillance Technology

How schools, police, health companies, and employers use surveillance technology that harms disabled people

Plain Language Report



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.

Report cover illustration

A dark blue / black background, with some lightly distorted paper textures.

Illustrated by Lydia X. Z. Brown, in light blue. 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.

Ableism And Disability Discrimination In Surveillance Technology

How schools, police, health companies, and employers use surveillance technology that harms disabled people

Plain Language Report

Acknowledgements

To Ali*, Alma*, Brandy Mai, Courtney Bergan, David Burick, and Wiley Reading: Thank you for sharing your stories with us.

To CDT staff Alexandra Givens, Ari Goldman, Cody Venzke, Eric Null, Greg Nojeim, Hugh Grant-Chapman, and Samir Jain: Thank you for reading this report and helping us make it better.

To disability rights/AI project advisory committee members Damien Patrick Williams, Karen Nakamura, and Rua M. Williams: Thank you for reading this report and helping us make it better.

To colleagues Corey Sauer, Cynthia L. Bennett, Jess L. Cowing, Os Keyes, and Shain A. M. Neumeier: Thank you for reading this report and helping us make it better.

To Avatara Smith-Carrington: Thank you for your early research on algorithms, risk assessment, and threat assessment.

* These people asked us not to use their real names. They wanted to stay private.

May 2022

Table of Contents

Introduction	5
Surveillance Algorithms in Education	10
Virtual test software: When algorithms watch students take tests	10
Automatic student surveillance	16
Recommendations	25
Criminal Legal System	26
Police algorithms that guess when and where crime will happen	27
Algorithms that decide if a person is a dangerous	31
When other algorithms use criminal records	33
Recommendations	36
Health Surveillance	37
Medications and medical devices that make sure people are using them	40
Algorithms that guess who has a disability or mental illness	41
Electronic visit verification (EVV) systems that track people with disabilities and their personal care attendants	42
Recommendations	45
Surveillance at Work	46
Algorithms that watch workers on the job	46
Company health and wellness programs	49
Recommendations	50
Conclusion	51

Introduction

New technology is everywhere. **Algorithms** are one type of new technology. Algorithms are computer programs. They can make decisions automatically.

Right now, students all over the world are talking about homework, gossip, and politics. And computer programs are watching what they search for online. Computer programs are watching what they post on social media. Computer programs are telling schools what students are looking at. And schools might punish students for what they look at.

Algorithms are making decisions about people's lives right now.

- Delivery workers are driving near you. Computer programs are watching where they go. Computer programs are watching how fast they are working. Computer programs are making decisions about their schedules and jobs.
- Lots of people are working from home right now. They are looking at their computers. And their computers are looking back at them. Computer programs time how long they get up to use the bathroom. Computer programs record their screens. Computer programs listen to them.
- Police use algorithms too. Computer programs are watching your neighborhood.

It might be happening where you live. It might be happening in another neighborhood close to you. Computer programs are deciding where police should go. Computer programs are deciding who police should pay attention to.

- Your phone might be keeping track of you. It might be paying attention to your heart beat or the oxygen in your blood. It might keep track of how much you walk. It might keep track if you are having a period. It might know what you eat. And your phone might be sending that information to many different companies. Your phone might even send that information to your boss. And computer programs might guess if you have a mental health disability too.

Algorithms are everywhere today. Algorithms are also getting smarter. Algorithms can guess if you'll like a restaurant. They can guess if you'll like a song. But not all algorithms are helpful or fair. Some algorithms are even dangerous.

Researchers and advocates have proved that algorithms can **discriminate**. Discrimination is unfair treatment. Sometimes, companies or the government are **biased**. Bias means unfair beliefs that hurt people. If companies or the government use algorithms, their algorithms can also be biased.

People, companies, and the government use algorithms to help make lots of decisions. They use algorithms to decide who can rent an apartment. They use algorithms to decide who to hire for a job. They use algorithms to decide who gets health care. And they use algorithms to decide who gets what ads.

Algorithms are in schools and workplaces. Algorithms in school and at work often watch people and pay attention to what people do. This is called surveillance.

Artificial intelligence (AI) is any computer program that can learn new information. AI can work on its own, like when your apps guess what ads you should get. There isn't a person deciding what ads you get, just the AI. AI can also work with people, like when a dating website gives you suggestions about who to talk to. You can decide to talk to the people or not. There are lots of types of AI.

Algorithmic decision-making is when algorithms make decisions. It can also be when algorithms make guesses about information. Some algorithms use AI. Other algorithms don't use AI.

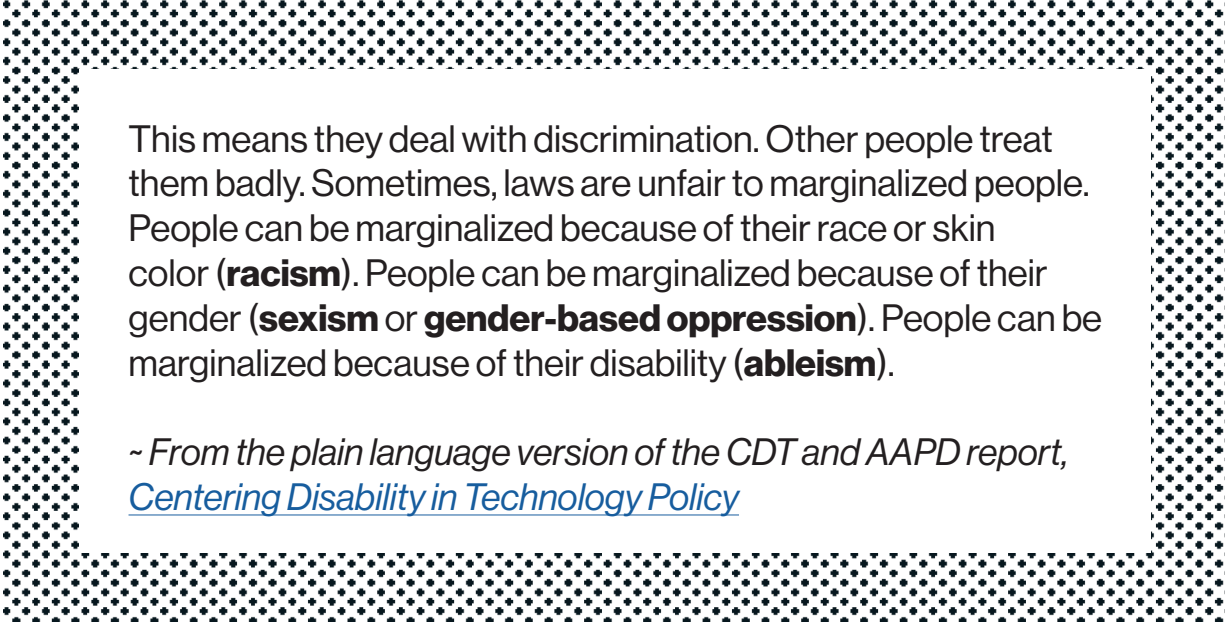
Automated decision-making is when algorithms use AI to make decisions on their own. Automated decision-making happens without people getting involved.

These three ideas are all connected. They have some overlap. But they're also different.

~ From the CDT and AAPD report, [Centering Disability in Technology Policy](#)

Automated decision-making can hurt disabled people. The algorithms can be biased against disabled people. The algorithms can discriminate against disabled people.

Disabled people are already **marginalized** in society.



This means they deal with discrimination. Other people treat them badly. Sometimes, laws are unfair to marginalized people. People can be marginalized because of their race or skin color (**racism**). People can be marginalized because of their gender (**sexism** or **gender-based oppression**). People can be marginalized because of their disability (**ableism**).

~ From the plain language version of the CDT and AAPD report, [Centering Disability in Technology Policy](#)

Some disabled people are also marginalized because of their gender or race.

But there isn't enough research about how algorithms hurt disabled people.

Algorithms use a lot of information (**data**) to make guesses and decisions. Data might show biased results. If the data is biased, the algorithm will also be biased.

For example, some landlords use an algorithm to decide who they will rent to. The tenant algorithm can look at people's credit scores. It can see if people have been kicked out of their homes (**evicted**). It can see if people have been arrested or gone to jail. But some people are more likely to have bad credit scores, get evicted, get arrested, or go to jail. This is because lots of landlords discriminate. It's also because the police discriminate. So poor people can be treated unfairly. People who have survived **domestic violence** (an abusive partner or family member) can get treated unfairly. People of color can also get treated unfairly.

This report talks about ways that algorithms hurt people in four areas. Specifically, this report talks about algorithms used for surveillance. Algorithms used for surveillance can watch what people do. They can also punish people. These algorithms can be dangerous for disabled people.

Here are the four areas:

1. Education (schools and colleges)
2. The criminal legal system (police, courts, and jails)
3. Health care
4. The workplace

In every section, we talk about examples of harmful algorithms. The algorithms can invade people's privacy. They are part of unfair rules and practices. They can make unfair systems worse. And they can backfire even when they're supposed to do something good.

Lots of people use the word "disability" to mean different things. We recognize that disability can mean a lot of things.

Some people are born disabled. Some people become disabled later in life.

Disabilities can affect how a person moves. Disabilities can affect what a person's body looks like. Disabilities can affect the five senses. Disabilities can affect people's feelings, thoughts, and learning. Some disabled people have **chronic illnesses**. Other disabled people have **mental illnesses** or **psychosocial disabilities**.

Lots of marginalized people are treated like something is wrong with their bodies or brains. So they have a lot in common with disabled people even if they're not disabled.

For our report, we followed the examples of the group Sins Invalid and the United Nations. Both groups say that being disabled also has to do with how you get treated by other people.

Surveillance Algorithms in Education

Students of all ages deal with surveillance. There are two main reasons schools use surveillance: (1) to stop cheating, and (2) to keep people safe.

Recently, schools started using surveillance technology. Some surveillance technology uses algorithms to guess who is cheating or going to hurt people. Surveillance algorithms can decide if people are suspicious. Schools use algorithms to decide who to look into or punish.

Surveillance algorithms are more likely to affect disabled students and students of color. They are even more likely to affect disabled students of color.

Surveillance algorithms invade students' privacy. They can treat students badly. And they can violate students' civil rights - breaking the law.

///

Virtual test software: When algorithms watch students take tests

Usually, a person watches students when they take tests. This person makes sure they follow the rules and don't cheat. This person is also in the same room, in-person, as the students.

But more and more schools watch students take tests **virtually**. There are two ways to give students virtual tests:

1. A software program can watch students take tests on their computers. The software program uses an algorithm. The algorithm can guess if students are cheating or doing something else wrong.
2. A real person can still watch, but **remotely** (on video from a different place). This person can look at a students' home through the computer camera.

After the COVID-19 pandemic started, lots of schools started giving students virtual tests.

Algorithms that watch students take tests can guess if they are breaking rules. They guess if students are looking at cheat sheets, talking to other people, or even getting someone else to take the test instead. The software program uses cameras and microphones. It can watch what students type and how they use computer mice. It can record what's on students' computer screens. The software program is keeping track of students' movement, speech, and behavior.

Students aren't allowed to talk out loud. They can't have other people or animals in the same room. They can't look at other computer programs besides the test. And they can't go off the camera to take breaks.

The software is more likely to think disabled people are breaking the rules. Even a person watching remotely might think disabled people are breaking the rules. A lot of disabled people have to take longer bathroom breaks or more bathroom breaks. Some disabled people use software that reads words out loud. Other disabled people use software that writes down what they say out loud. And the software can make people with anxiety even more anxious.

A group called the National Disabled Law Students Association wrote a report that talks about how algorithms discriminate against disabled students. They give a lot more examples of disabled students dealing with discrimination from the software.

Courtney Bergan is a white person with more than one disability. They have post-traumatic stress disorder (PTSD), a disability that happens after surviving one or more awful experiences. They have Ehlers Danlos Syndrome, a disability that affects all the organs in the body. And they have low vision.

Courtney took a test required to apply for law schools. They had to use a software program where a person watched them remotely. Courtney was supposed to get accommodations, which are changes that are made so disabled people get fair treatment. They were supposed to have extra time. They were also supposed to have extra breaks to use the bathroom and take medication.

But the person watching remotely said Courtney wasn't allowed to take breaks. The remote person said Courtney couldn't use the bathroom or take their medication. Courtney ended up clicking random answers just to finish faster.

Courtney is also nervous about taking other tests. One of their disabilities means they have uncontrolled eye movements. They're worried the software will think they're cheating because of how their eyes move.

Some software that watches students take tests use algorithms to recognize faces too. This can be bad for disabled people and people of color.

People giving tests want to make sure that the right people are taking the tests. They might use software that matches a person's face to a picture. One software program makes students look at their computer camera so it can tell if there is a face. Then it uses face recognition software to make sure the same person stays at the desk the whole time.

Face recognition software might have a hard time recognizing some disabled people. Some disabled people have conditions that affect what their faces look like. Some disabled people have gotten surgeries on their faces. Some disabled people use mobility equipment. Algorithms might not understand how to recognize people with unusual skin, eye colors, or growth on their bodies. And one research study showed that blind people had a hard time taking selfies good enough for face recognition software.

Face recognition software is often trained on biased data. There aren't enough disabled people or people of color in the data. A lot of research shows that face recognition software is bad at recognizing people of color, especially if they are very dark-skinned. In 2018, one important project called Gender Shades found out that face recognition software was especially bad at recognizing dark-skinned women. A year later, the government agency National Institute of Standards and Technology (**NIST**) said that 189 different face recognition algorithms were worse at recognizing women of color.

People of color are often more likely to have a disability. So racial discrimination will end up affecting a lot of disabled people of color too.

But there are problems even when algorithms get better at recognizing people of color and women. In 2022, NIST said that some algorithms were getting better at recognizing women of color. But NIST doesn't test if the algorithms can recognize disabled people. And even if the algorithms are 99% accurate, they will still get it wrong for thousands and thousands of people. And that can be dangerous.

For example, Kiana Caton is a Black woman who went to law school. She took the **bar exam**, a test you take to become a lawyer. Kiana had to deal with

face recognition software for the bar exam. She knew the computer program might not recognize her face because of her dark skin. So she had to shine an extremely bright light on her face for two straight days. That light sometimes gave her headaches. The light might have made Kiana extra anxious. The pain and anxiety would make it hard to focus.

So Kiana was treated unfairly. She was less likely to pass, but not because she didn't know the answers. She was less likely to pass because she was dealing with pain and anxiety.

Some groups have complained about face recognition software for tests.

One group, the Electronic Privacy Information Center, made a civil rights complaint. They said that virtual test software invaded students' privacy. They also said that virtual test software was unfair and not truthful.

The complaint had three main issues:

1. Virtual test software collects too much information about students.
2. Virtual test software uses unfair, secret algorithms.
3. Virtual test software companies lie about how good their face recognition software is.

Three disabled people in California filed a separate court case. They went to court over virtual test software in 2020. They were all trying to take the bar exam to become lawyers. But the state wouldn't accommodate their disabilities with the virtual test software. The state said they had to take the test in-person, even though it was during the COVID-19 pandemic.

California's virtual test software discriminated against a lot of disabled people:

- The software wouldn't let people take bathroom breaks, even if they had stomach issues.
- The software wouldn't let people take the test on paper, even if they had problems with looking at screens.

Some software that watches students take tests use algorithms to recognize faces too. This can be bad for disabled people and people of color.

- The software wouldn't let people use scratch paper, even if they needed extra writing space.
- The software wouldn't adjust for people who needed extended time.
- The software wouldn't understand people who used programs that read text out loud, or write down what they say.

The disabled people in this case even asked the state to invade their privacy more. They said the state could use a second computer camera to watch them. They said they could explain out loud why they were taking extra breaks. They even said they could take pictures of their bathrooms. But the state said no. The state said they had to take the test in-person no matter what. The state didn't care that disabled people have higher risks from COVID-19.

Other states made people take the bar exam with virtual test software up through February 2022.

Virtual test software can break the law.

Virtual test software can violate the Americans with Disabilities Act (**ADA**). The ADA says that any government program, almost every school, and most companies have to accommodate disabled people. They aren't allowed to discriminate against disabled people. So if virtual test software discriminates, it might be illegal.

Virtual test software can also violate laws that protect people who buy and use stuff, like the Illinois Biometric Information Privacy Act (**BIPA**).

College students at Northwestern and DePaul Universities in Illinois took their colleges to court in 2021. They said the colleges violated BIPA. Both colleges made students put virtual test software on their computers. The software programs used microphones, cameras, and face recognition software to watch what students typed and see if students looked away. Students had to use the software to pass their classes. But the colleges didn't tell students what the software was doing. They didn't let students put limits on the data.

As of spring 2022, the students at Northwestern were waiting to go to court. The college is trying to make the case go away. The college says the school doesn't have to follow the BIPA law because it is a "financial" institution.

Automatic student surveillance

Lots of students go online to study, meet people, participate in the community, and get involved in politics. They will likely deal with automatic surveillance at home, on computers from their schools, and while at school or college.

Automatic surveillance will likely hurt students with disabilities. Disabled students deal with very high rates of punishment in school. Disabled students are also more likely to need assistive and adaptive technology that helps them.

The National Council on Disability has said that disabled students of color are punished even more in school. This is because of disability discrimination combined with racial discrimination. This means that disabled students of color are more likely to end up in jail later.

The Center for Democracy and Technology interviewed special education teachers and families of disabled students. They also said they were worried about schools using automatic data to make decisions about students. 71% of special education teachers were worried about schools using biased data to make decisions that could stop students from succeeding in school or at work. 64% of special education teachers were worried about schools sharing student data with police.

Research shows that being punished in school makes going to jail more likely. So students and advocates are worried about schools using automatic surveillance. Schools are using automatic surveillance to watch students on

social media and watch what students do at school or at home to make guesses about who will be violent. (This is called a **threat assessment**.)

Threat assessment: When software guesses who will be violent

Schools say they use threat assessment software to make school safer and stop violence. Software companies like ALiCE, Crisis Go, and USA Software sell programs to schools with questionnaires, charts, and algorithms that use data. These programs guess which students are threats. Threat assessment programs might ask people to look at a student's appearance, interests, and friends. Another company, called OnGuard, sells software that keeps track of students' social media posts. This software keeps track of students' locations and it reads words in their posts.

Threat assessment software is supposed to be used by a team of people. The team is supposed to think about more information (**context**) that can explain why a student might be acting weirdly or differently.

Disability discrimination and racial discrimination often overlap.

Threat assessment can hurt disabled students and students of color. Both groups are more likely to get looked at by a threat assessment team. Some research says that threat assessment teams aren't racially biased. But other research says that disabled students are more likely to get looked at by threat assessment teams. Other research also says that schools with more students of color are more likely to have threat assessment teams.

Automatic threat assessment and individual people might make mistakes with disabled students and students of color too. They can have racial bias and disability bias. They might not understand how disabled students and students of color talk. They might assume disabled students are being anti-social, inappropriate, or scary because of how they talk or what they're interested in. They might assume that Black students are scary, disrespectful, or violent if they are using Black American English/African American Vernacular. And they might assume that disabled Black people are even more violent or aggressive. Then those students would be more likely to get punished.

For instance, a school in Oregon treated a white autistic student in high school as a shooter waiting to happen. The school thought the student was dangerous even though he never made any threats.

There is a lot of bias about people with mental health disabilities (like depression and bipolar) and developmental disabilities (like autism). One ableist idea is that people with mental health disabilities or developmental disabilities are more likely to be violent.

For instance, a school in Oregon treated a white autistic student in high school as a shooter waiting to happen. The school thought the student was dangerous even though he never made any threats.

Another school in New Mexico sent a Black autistic student in elementary school to a threat assessment team. The student had a meltdown where he bit and hit one teacher. Disabled students were 56% of all the people sent to the threat assessment team in the school district. But disabled students were only 18% of the whole population.

Threat assessments could cause racial or religious discrimination, too. Threat assessments could also make racial or religious discrimination worse.

For instance, Countering Violent Extremism is a police program that discriminates against Arab and South Asian Muslim youth. This program uses undercover police to try to find terrorists. They assume that Arab and South Asian Muslim youth are more likely to be terrorists because of bias.

Other police departments try to guess which youth are in gangs. They often discriminate against Black and Latinx youth. These police departments assume that Black and Latinx youth are more likely to be gang members.

28% of Muslim students in New York City public schools said they were profiled and stopped by the police. 28% of Muslim high school students in California said they were discriminated against by teachers and administrators. Black students were almost 10% of the students sent to a threat assessment team. But Black students were less than 3% of the whole population.

Racial and religious discrimination can also cause more mental health stress in marginalized students.

Social Media and Off-Campus Monitoring: When schools watch what students do at home

Schools use software to read what students write on social media. Schools also use software to watch what students do online. This software is supposed to guess if students are going to be violent. 81% of teachers said their schools use some type of monitoring software. 43% of the group (almost half) said their schools use the monitoring software to punish students.

Marginalized students can get punished more. Algorithms might look at how they talk, what they look like, and what they post online. When the algorithms guess they will be violent, schools will pay closer attention to what they do.

But research shows that software is bad at understanding social media. The algorithms don't understand context. For example, a student could say "I bombed that test" or "I want to try a new bath bomb." But the algorithm would just read the word "bomb." Then the algorithm would flag the post as a threat.

Ali is a disabled student of color. They dealt with surveillance at their school. They also got punished.

It started when they stood up to a biased preacher. Another student made up that Ali was stalking a professor and wanted to hurt the professor. Ali was angry because the professor tried to take sexual advantage of a student. But Ali wasn't even going to say something to the professor.

Students were watching everything Ali did online. Sometimes they tried to get Ali to talk about their feelings. Then they would share what Ali said with the college's administrators. They would make up lies that Ali was threatening people.

One time, someone said Ali should go out "with a bang." They meant throw a big party and make a mess. But the school said Ali was threatening to burn down the building.

Students said Ali was scary for playing video games with guns and looking at gun pictures. Someone said Ali only went to the gym to get ready to fight people. Someone else said Ali was stalking another student because Ali said they saw the student on campus.

Ali got lawyers. The college wouldn't share the evidence against Ali though. The college tried to punish Ali with no real evidence. The college tried to kick Ali out. But Ali fought back. Ali was allowed to go back to school. But the school banned Ali from going to campus for a couple years.

Ali decided to go to a different school.

Some software reads what students write online. But the algorithms don't always understand what students write. The algorithms are bad at understanding people who don't use standard English. That means the algorithms won't understand people who aren't fluent in English. They won't understand people who use Black American English. And they might not understand people who have speech disabilities.

Researchers tested a hate speech algorithm. The algorithm was 1.5 times more likely to say Black people's posts were hate speech than white people's posts. The algorithm was 2.2 times more likely to say posts in Black American English were hate speech than posts in standard English.

Other researchers asked people to find hate speech. The researchers showed the people posts from a hate speech database. The people almost always disagreed with each other. Only 5% of posts got a majority of the group to say they were hate speech. Only 1.3% of the posts had the whole group saying they were hate speech.

People write algorithms. People also decide what to do when an algorithm makes a guess or a decision. So when people are biased or disagree, it will affect the algorithms.

Monitoring software uses data to learn. That data can be biased. Often, data has gender, race, or disability bias. Algorithms that use this data will then also be biased.

For example, students and teachers might be more likely to say that Black, Muslim, or disabled students are being threatening. So an algorithm might also learn to say Black, Muslim, or disabled people's posts are threatening. And then teachers and administrators will think that marginalized students are problems. That may not be accurate.

This problem is worse during the pandemic. A lot of poor students use computers given by their schools. When schools give students computers, they might put surveillance software on the computers. 71% of teachers said their schools use monitoring software on computers given by the schools. But only 16% of teachers think that families use monitoring software at home.

The monitoring software might guess if students are threatening. It might guess if students want to die by suicide.

Schools sometimes think it's okay to use software if people check the results. But involving people doesn't make bias go away. Scholar Kimberlé Williams Crenshaw said Black girls in New York were almost 10 times more likely to get suspended than white students in 2011-2012. Disabled students are three times more likely to be arrested than nondisabled students. Almost 80% of students restrained (held or strapped down) were disabled. And up to 85% of youth in youth prisons were disabled. Humans helped make these biased decisions.

On-campus surveillance: When schools are watching you every minute on school property

Lots of schools use surveillance technology to watch students. Schools and colleges think surveillance technology makes students safer. Schools also have police. They use metal detectors to look for weapons. They use microphones to listen for "aggression." They use face recognition technology to see who is at the school and what they are doing. They use cameras to see if people are supposed to be at the school. And they use software to make guesses about people's tone of voice, feelings, and attitudes.

Surveillance technology tracks a lot of information about students and people who work at schools. And sometimes schools already discriminate because of race, gender, and disability. So surveillance technology can discriminate too.

Schools use microphones to listen to people talking. These microphones are connected to a computer program. The computer program uses an algorithm to guess if people are scared, aggressive, or angry. If the algorithm thinks someone is very scared, aggressive, or angry, it sends an alert. The alert tells schools where the noise is happening. Then school workers can decide what to do. For example, the software listens for screaming, threats, and fights.

Schools aren't the only place using these microphones. Hospitals and prisons use them too.

But the people and computer programs listening to the microphones can be biased. They might decide to go after students based on stereotypes about

gender, disability, or race. Some disabled people have a hard time controlling their voices. This happens a lot for autistic people, deaf people, and people with cerebral palsy. Other disabled people get angry and frustrated when they don't have the right support, or when they're being bullied. This happens a lot for people with mental health disabilities and learning disabilities.

The microphone software can also get it wrong. The news group ProPublica found out that one microphone software program was wrong hundreds of times. The algorithm thought that laughing, coughing, and closing locker doors were threatening noises. This could hurt disabled students who make sudden noises or can't control what they sound like. This happens a lot for people with Tourette's, cerebral palsy, and ADD.

Other schools use face recognition technology to watch students. But face recognition technology can get it wrong too. It might not recognize disabled people or people of color.

Researchers at the University of Michigan are worried about face recognition technology in schools. They think it will discriminate against Black and Brown students. They are worried that Black and Brown students will get punished more.

In 2020, Lockport City schools in New York were the first to use face recognition technology. They got the technology to try to stop school shootings. But less than a year later, journalists found out the technology company was lying. The company that made the software said it was accurate and reliable. But the software thought broom handles were guns. The software was four times more likely to get it wrong when identifying Black men than white men. And it was 16 times more likely to get it wrong when identifying Black women than white men.

Face recognition software might get it wrong for disabled people too. It might not recognize disabled people's canes, crutches, or oxygen tanks. And it might not recognize disabled people's bodies.

Surveillance technology might not stop violence at all. Shootings are scary. But they happen way less often than other kinds of violence in schools. And face recognition technology only tries to guess if someone is allowed to be at

a school. If a shooter is a student, the face recognition technology won't stop them.

Schools should do their best to stop shootings from happening. But automatic surveillance technology won't work. And even worse, automatic surveillance technology will hurt people.

Recommendations:

- Schools should talk to disabled people and other marginalized people before buying surveillance software. They need to make sure their software isn't biased or discriminating. They should hire people to double check the software to make sure it works.
- Schools should check the software regularly and often. They should check to make sure it isn't biased or discriminating.
- Schools should be up front about how the software works. They should make sure students and parents know about the software. They should tell students and parents how the school uses the software. And they should say how they're trying to stop bias.
- Schools should understand it's hard for disabled students to ask for accommodations. Schools should make it easier to ask for accommodations. They should treat disabled students with respect. They should teach staff how to be respectful.
- Schools should not force students to deal with surveillance all the time. Schools should explain how surveillance software works. They should let students and families make choices. They should let students say no. And they should give students covers for their computer cameras.
- The Department of Justice and Department of Education should tell schools they have to follow the law. Important laws like the Americans with Disabilities Act (Title II), Rehabilitation Act (Section 504), and Individuals with Disabilities Education Act all protect students. Software has to follow the law too.

Criminal Legal System



Police, courts, and prisons use algorithms too. These algorithms can get more people arrested and sent to jail. Police use software to guess where crimes will happen and who will commit them. Judges use algorithms to help decide who to release on bail. These algorithms can ruin people's lives. Landlords might automatically say no if someone has a **conviction** record. (A conviction is when someone is found guilty of a crime.) Landlords might even say no if someone has an arrest record, even if they didn't get convicted. If people can't get a place to live, they can become homeless.

A lot of researchers and advocates talk about how algorithms related to crime are racist. Some advocates say that the algorithms can be biased because of gender, religion, or class. (Class is how much money and privilege a person or their family has.) The algorithms can also discriminate against disabled people too. Police algorithms might think disabled people are more likely to be criminals.

A lot of police algorithms discriminate against people of color and poor people. People of color and poor people are more likely to be disabled. Disabled people are also more likely to be poor. So algorithms that discriminate against people of color and poor people also probably discriminate against disabled people.

Police algorithms that guess when and where crime will happen

Police started using data to guess where crime will happen a long time ago. In 1994, the New York Police Department (NYPD) started collecting lots of data about crime. They used a system called CompStat. Then the NYPD pressured police officers to arrest more people. They wanted police officers to stop more people on the street or in their cars. The NYPD started putting all the information they got from these arrests and stops into CompStat. They could tell police officers all the information about any person. CompStat could say if someone got arrested. CompStat could say if someone had a conviction record. CompStat could say if someone was on probation or parole. (That means a court said they had to report to an officer and follow a lot of rules instead of going to jail.) Police officers could look at CompStat and get all this information right away.

Now, even more police departments use similar computer software. They use software to collect information about crime. And they use software to guess where crime will happen. Lots of police departments also use **biometric** software programs. Biometric programs use information about people's bodies. Face recognition software is one example of a biometric program. Police departments use biometric programs to identify people. They also use biometric programs to guess who will commit crimes.

The Los Angeles Police Department (LAPD) used to have two software programs. Their programs both used algorithms.

In 2008, LAPD started using a program called Operation LASER. Operation LASER said its algorithm could figure out who committed lots of crimes. The algorithm gave people points. People got points for being on parole or probation. People got points if the algorithm thought they were in a gang. They got points for being in a gang even though the list of gang members was wrong a lot. They even got points if police officers only stopped them. The algorithm said people with a lot of points probably committed lots of crimes.

LAPD used another algorithm that guessed where crimes would happen. Police officers would go to those places. They would go even if there wasn't a lot of crime happening. LAPD could work with government lawyers to put people in jail. LAPD could even work with government lawyers to get people kicked out of their homes. The government lawyers could tell landlords to watch their renters.

Advocates are worried that police algorithms can make racism worse. Sometimes the algorithm says a neighborhood has more crime. Sometimes the algorithm says specific people are probably criminals. The algorithm will make these guesses based on who is already getting arrested and going to jail.

The government lawyers could also tell landlords they should kick people out.

An independent office looked at the LAPD algorithms. It said Operation LASER was like surgery “to remove tumors.” This quote shows the government’s real attitudes. It shows that the police didn’t respect people with lots of points. It shows that the police thought people could be bad like a cancer tumor.

Chicago’s police department also started using software in 2013. This software program looked at people’s arrest records. It also looked at who people’s friends were. Then the algorithm guessed if people would be involved with a shooting. A civil rights group called Upturn said that the list made no sense. It said one-third (33%) of all people on the list weren’t victims of crimes. They didn’t even have arrest records. But people on the list were more likely to get arrested later.

In 2019 and 2020, LAPD stopped using the two main algorithms. Lots of advocates helped make that happen. They took LAPD to court because a lot of people in Los Angeles were worried about the algorithms. They thought the algorithms were biased.

Chicago also stopped using its algorithm in 2020.

But advocates know LAPD and Chicago are still using police algorithms. LAPD and Chicago are using police algorithms even though they were supposed to stop.

There is a lot of racism in the criminal legal system. People of color don’t commit more crimes than

white people. But people of color are more likely to get arrested and go to jail. Police, government lawyers, and judges can be biased. But even if individual people aren't biased, lots of laws are biased. And if lots more people of color are going to jail, that's a sign that there is bias.

Advocates are worried that police algorithms can make racism worse. Sometimes the algorithm says a neighborhood has more crime. Sometimes the algorithm says specific people are probably criminals. The algorithm will make these guesses based on who is already getting arrested and going to jail.

More Black, Native, and Latinx people get arrested than white people. But there isn't always more crime in Black, Native, and Latinx people's neighborhoods. Police might just be biased.

Algorithms might not have complete information either. Not every victim makes a report. And sometimes police don't look into people's reports.

And algorithms might not always be right. People can get arrested even if they're innocent. And people can even get convicted if they're innocent. Sometimes people are pressured to plead guilty so they don't have to go to jail for a long time. Sometimes people are pressured to give false confessions. And sometimes police use bad evidence against people.

So algorithms shouldn't rely on arrest or conviction records to guess who will commit crimes.

And advocates are worried about police algorithms no matter what activities are illegal. (Some advocates also say that some laws are wrong, like making it illegal to have a drug addiction.)

Some cities agree with advocates. They think the algorithms are biased too. Some of them want to stop using police algorithms:

- In December 2020, Oakland, California banned police algorithms and biometric surveillance.
- Santa Cruz, California and New Orleans, Louisiana banned police algorithms and face recognition software.

- Bellingham, Washington voters banned police algorithms and face recognition too.

Police algorithms can discriminate against disabled people, too. They are especially dangerous for disabled people of color. People of color are more likely to be disabled. Disabled people are also more likely to be poor.

Police tend to arrest more people in neighborhoods with lots of poor people and people of color. That means police are arresting lots of disabled people already. Police algorithms might send even more officers to neighborhoods with more disabled people.

Police algorithms also try to guess who is a threat. The algorithms might use information related to disability. They can use this information even if it's unrelated to who is a threat.

For example, the Pasco County Sheriff's Office in Florida started making lists of kids. They were making a list of kids they thought would be criminals. They put students on the list for getting D grades in school, being absent a lot, or dealing with domestic violence at home. Disabled students are more likely to get bad grades if they're not getting support. Disabled students are more likely to be absent if they have chronic illnesses. And disabled students are more likely to be abused at home.

It might not be possible to fix the algorithms. It might not even be possible to make them better. And bad algorithms will cause more disabled people to be arrested and put in jail.

- People with developmental disabilities are at least 7 times more likely to deal with police.
- The U.S. Department of Education says that disabled students are more likely to get arrested in school. Black and Brown disabled students get arrested even more.
- Disabled people are 44% more likely to get arrested. This is especially bad for people with mental disabilities.

- Lots of disabled people get hurt by the police. Police might not understand disabilities. Police might think autistic people and mentally ill people are on drugs. Police might think Black people with canes or wheelchairs were involved with violent crime. And police might think deaf people are resisting when they can't hear.

Fair governments shouldn't use police algorithms that discriminate. We have to talk about racism in the criminal legal system. We also have to talk about ableism in the criminal legal system. Biased algorithms won't stop unless governments stop using them.

Governments have to work with advocates for racial justice, disability rights, and disability justice. Policy leaders can stop paying for biased algorithms. And they can give money to community support and services instead. Policy leaders should give money to services and programs led by marginalized people. This could mean education programs, job programs, mental health support, and social work.

Algorithms that decide if a person is a dangerous

Some algorithms decide if a person is dangerous. This means if a person is a risk to other people.

Judges use **risk assessment** algorithms to decide if people should go home after getting arrested. The judges want to know if people will come back to court. They also want to know if people will commit more crimes.

Parole officers and probation officers also use risk assessment algorithms. They want to know if someone should get out of jail. They want to know if someone will be dangerous.

Risk assessment algorithms are supposed to be fair. They're not supposed to be biased. But researchers say risk assessment algorithms can be biased. Risk assessment algorithms guess who is dangerous. They make guesses with people's information and criminal records. But criminal records can show bias. People of color and disabled people are more likely to get arrested and go to jail.

In 2016, the news group ProPublica looked at Broward County, Florida. Judges used a risk assessment algorithm called COMPAS. They used COMPAS to decide if people should get bail. But COMPAS was two times more likely to say Black people would commit crimes than white people. And COMPAS was more likely to say white people were low risk no matter what.

A man took Wisconsin state to court in 2016 too. Wisconsin judges used COMPAS to help decide people's punishments. The court decision said judges could keep using COMPAS. But judges had to get a warning before using the algorithm. And judges couldn't use the algorithm to decide if people should go to prison. Judges also couldn't use the algorithm to decide how long people should go to prison.

Risk assessment algorithms can discriminate against poor people and people of color. They can also discriminate against disabled people. Risk assessment algorithms don't say they use race, money, or disability to decide if someone is dangerous. But they look at information related to race, money, and disability. Here are some examples:

- Education: Disabled people might be discriminated against in school. Disabled people might not get accommodations or services.
- Arrest or conviction history: Disabled people are more likely to get arrested. Disabled people are more likely to go to jail. This is even worse for disabled people of color.
- Work history: Disabled people are more likely to be jobless. Disabled people might deal with hiring discrimination too.
- Housing: Disabled people are more likely to be homeless. Disabled people are also more likely to be poor. It's harder for poor people to stay living in one place.
- Community and family support: Disabled people might not have partners or children. Disabled people might be dealing with discrimination from child welfare. Some disabled people get their children taken away because of stereotypes about disabilities. Disabled people might not have supportive families. Some disabled people might have cut off abusive families.

It's hard for a risk assessment algorithm to be fair and accurate. People with criminal records are the most likely to get arrested again. But criminal records can show lots of bias. Lots of activities are crimes, even if some of them shouldn't be (like being addicted to drugs). Police can decide who to arrest, and they might be biased. Government lawyers can decide how to go after people. Lots of people are wrongfully convicted. And people of color and disabled people get arrested and go to jail more often.

So lots of algorithms use criminal records to guess who will commit crimes. But these algorithms won't always get it right.

And using risk assessment algorithms also sends other messages. Governments are saying the criminal legal system is working fine. But the algorithms don't solve the real problems. The algorithms can't figure out how to stop violence. The algorithms can't stop police from being biased either.

When other algorithms use criminal records

If you get a criminal record, it will follow you for a long time. It will affect many parts of your life.

Landlords use tenant algorithms to decide who to rent to. These algorithms might use criminal records. Employers use algorithms to decide who to hire. These algorithms also might use criminal records. And people on dating sites might look at criminal records too.

Criminal records can make it hard to get benefits. And they can make it harder to get a loan too.

It's hard for people to get jobs or find housing after getting out of prison. But algorithms can make it hard for people even if they only were arrested once. And they can mix people up too.

Disabled people are more likely to get arrested and go to jail. So algorithms that use criminal records can discriminate against disabled people.

Carmen Arroyo was renting an apartment. She wanted her disabled son Mikhail to move in with her. So her building did a background check on Mikhail. They used a software company called CoreLogic. CoreLogic automatically denied Mikhail.

CoreLogic said Mikhail had a criminal record. But Mikhail was only arrested once for shoplifting. It was a long time ago. He wasn't even convicted. And his disabilities would make it very hard to shoplift again.

Mikhail couldn't move in with his mother. So Mikhail was sent to an institution for a whole year.

Carmen took CoreLogic to court. Carmen and Mikhail are still waiting for a decision.

Tenant algorithms can break the law. The Fair Housing Act says landlords can only use information about convictions. Landlords can use convictions to say no to renters. But landlords can only use convictions related to the situation. For example, landlords could say no to someone who was convicted of robbing people in their last building.

But tenant algorithms sometimes use arrest records. And lots of people get arrested but not convicted. Worse, tenant algorithms might not give landlords enough information to make a careful decision. The algorithm might just say someone has a record. But then the landlord doesn't know what kind of record. The landlord doesn't know any details about the record. So the landlord can't make a fair decision.

Landlords can say no to lots of people with convictions. But that can discriminate against people of color and disabled people. Both groups are more likely to get arrested and go to jail. So using convictions can stop more disabled people and people of color from getting housing.

Tenant algorithms might use any police records. This can be bad for victims and survivors of domestic violence. Remember that domestic violence is abuse from a partner or family member. It is illegal to discriminate against victims and survivors of domestic violence. But lots of landlords call police on victims of domestic violence. The landlords say the victim is a problem. This can get the victims kicked out. And it can make it harder for victims and survivors to get housing later.

Other algorithms use public records too. Lots of dating apps ban people with conviction records. But the dating apps might have the wrong records. And they don't always tell people why they're not allowed. That means people can't ask the app to challenge or fix a mistake.

Using conviction records can be risky. It can also be unfair. And it can be discrimination. People in prison are more likely to be disabled. So banning or rejecting people with conviction records means banning or rejecting lots of disabled people. It also means banning or rejecting lots of other marginalized people too. Algorithms that use conviction records assume all people with convictions are dangerous. They also assume that all convictions are right. And they are still punishing people even after they get convicted.

Recommendations:

- Police departments should stop using police algorithms that discriminate.
- Courts need to make sure people and their lawyers understand risk assessment algorithms. Courts need to make sure people and their lawyers can point out mistakes in the algorithm.
- Employers and landlords have to stop using arrest records in background checks.
- Employers and landlords should be very careful with information about evictions (getting kicked out of housing) and convictions (being found guilty of crimes). They should only use very recent records. They should only use records related to the situation. And they should finish going through a person's job or housing application to look at records. This helps give people a fair chance.

Health Surveillance



Health companies use algorithms for surveillance too.

In January 2022, news group Politico found out that a mental health hotline was sharing people's information. Crisis Text Line is supposed to be a private hotline. People can contact Crisis Text Line if they are scared, angry, or upset. People usually contact Crisis Text Line if they are thinking about hurting or killing themselves.

Crisis Text Line was giving people's information to a private company. The company designs algorithms for customer service. Crisis Text Line said it took names and personal information out of the data they shared. But people contact Crisis Text Line because it's supposed to be private. Advocates like Kendra Albert at Harvard said that sharing any information goes against Crisis Text Line's purpose.

Lots of advocates told Crisis Text Line it was wrong. They spoke out in public. Less than a week after Politico got the news, Crisis Text Line stopped the sharing.

Disabled advocates want to stop ableism, or disability discrimination and bias. One ableist idea is that all disabilities are health problems. In other words, lots of people think that all disabled people are sick all the time. This isn't true for every disabled person. But disabled people are more likely to

deal with lots of doctors. Disabled people are more likely to deal with health problems. And lots of people think that disabled people aren't healthy. So health information is extra important for all disabled people.

Lots of companies invade disabled people's privacy. They pressure disabled people to give up personal information. And they don't tell disabled people what they're doing with the information. That means disabled people might not understand their rights.

Disabled people also get stuck in bad situations. Disabled people need to use health apps, get benefits, use connected devices, and set up medical treatment. But disabled people have to give up a lot of privacy to do all those things. And disabled people have to give up their privacy without knowing all the information. This isn't an informed choice. This is a forced choice. And it can be hard to look for different doctors or services. Lots of doctors and services discriminate. And not enough take insurance, including Medicaid.

Disabled people might also need to ask for help to use an app or device. They might have to share their information with someone who helps them. People with disabilities can't use every app or device. A lot of apps and devices are inaccessible. When people with disabilities need to get help, their information might not be private anymore. So people with disabilities have to choose between keeping their information private and getting help.

Disabled people deal with lots of invasions of privacy. Companies keep track of lots of data about people with disabilities. Here are some examples of privacy issues:

- Medications and medical devices that make sure people are using them
- Algorithms that guess who has a disability or mental illness
- Electronic visit verification (EVV) systems that track people with disabilities and their personal care attendants

The International Digital Accountability Council published a new report about health apps. They looked at apps for pregnant people, new parents, people who **menstruate** (bleed once a month), mental health disabilities, and fitness.

- 82% of the apps told people they collect personal information. But only 54% told people they collect health information.
- 21 fitness apps, 15 pregnancy and menstruation apps, and 6 mental health apps all asked for people's exact location.
- 2 apps shared people's private health information, phone numbers, and emails without protecting the information.
- 2 apps had no privacy policy at all.

The International Digital Accountability Council (**IDAC**) said that federal laws aren't good enough to protect people. Our laws say companies have to tell people what they are doing (**notice**). And the laws say companies have to get permission (**consent**). But IDAC said that a lot of apps just give people lots of complicated information. The information is hard to read and understand. So that's not good notice. And IDAC said a lot of apps just make people click checkboxes to give permission. But people don't know what the checkboxes are. And the apps don't really tell them.

Medications and medical devices that make sure people are using them

Doctors want to make sure people follow instructions. They want to make sure people take medication. And they want to make sure people use medical devices. But some medications and medical devices automatically track what people are doing.

Automatically tracking what people are doing isn't always good. It might not be helpful. And it might make people worried about getting treatment.

In 2017, the Food and Drug Administration approved a new pill called Abilify MyCite. This is an antipsychotic medication. Each pill has a sensor in it that can tell if someone has taken the medication. This was the first time the government said it was okay for a pill to have this sensor.

The company that made Abilify MyCite thinks that people with mental illnesses are unreliable. It thinks people with mental illnesses might not follow instructions. But people with mental illnesses deserve choices. People with mental illnesses can choose to follow instructions. People with mental illnesses can choose to take a risk. And people with mental illnesses can check with another doctor. But people with mental illnesses should get privacy too.

There are medical devices that track people too. Some people with diabetes use devices that pay attention to their blood sugar. Some people with sleep apnea use machines that pay attention to their sleep and breathing. The devices can be outside a person's body, or they can put a sensor inside the body. Some companies let doctors get the data from the devices remotely.

These devices might help a lot of disabled people. But advocates are worried about protecting people's privacy.

Disabled people can want medical treatment and privacy. But doctors and insurance companies have a lot of power. So disabled people might not get a real choice about their treatment. Disabled people could be forced to use technology they don't want. This is especially bad because disabled people are more likely to need medical treatment. But disabled people are less likely to have options for doctors and treatments.

And other companies might get people's information too. Companies can use health information to make guesses about people's lives. Companies can use health information to change people's services. Companies might use health information to discriminate. Insurance companies might use health information to charge people extra money.

In 2019, a news group found out that a pregnancy app was sending information to people's employers. People who had trouble getting pregnant might not want to share that information. But their employers were getting all this information about them.

Algorithms that guess who has a disability or mental illness

Algorithms can guess who has a disability or mental illness.

Researchers did an experiment with an algorithm about mental illness. This algorithm looked at people's Facebook posts and private messages. Then it guessed if the people would get diagnosed with a mental illness. The algorithm said a lot of the people would get diagnosed with a mental illness. And the algorithm was right. Those people got diagnosed a year later.

Researchers did another experiment with an algorithm about mental illness. This algorithm looked at people's Twitter posts. The algorithm looked at the tone of voice. It looked at what people talked about. Then the algorithm guessed if people would get diagnosed with depression or post-traumatic stress disorder. The algorithm was right. It even guessed right using months-old Twitter posts.

Big tech companies want to use these algorithms too. They do a lot of research for their companies.

Facebook already uses an algorithm to see if people's posts are about suicide. Facebook even sends that information to emergency services without permission.

So some people in the disability community avoid talking about suicide on Facebook. Or they ask friends not to report their posts for suicide. They don't

want Facebook to limit their accounts. They want help and support from their community.

In September 2021, Apple researchers started looking into iPhone sensors. They are working with university researchers to make algorithms. They want to make algorithms that can figure out if people have depression, dementia, and other disabilities.

Algorithms that track what people say online can be scary for disabled people. A lot of disabled people use social media to meet people and get support. People who feel suicidal are often disabled, especially if they feel suicidal a lot. Lots of marginalized people can feel suicidal too. And it's not good if marginalized people are afraid to ask for help.

Advocates should also be worried about algorithms that guess who has mental illnesses. Those algorithms could share information with landlords, employers, dating sites, or other companies.

Electronic visit verification (EVV) systems that track people with disabilities and their personal care attendants

A lot of disabled people have to deal with electronic visit verification (EVV) technology. This technology tracks people with disabilities and their personal care attendants (PCAs). It tracks what hours PCAs are working. It tracks where PCAs and people with disabilities go. EVV technology makes workers pay attention to every little thing they do. This is supposed to keep people honest.

But EVV technology is another system that assumes poor people and workers are liars who need to be watched.

Federal law says EVV technology is required for people getting Medicaid services. People getting PCAs with Medicaid had to start using EVV by January 2021. And people getting Home and Community Based Services from Medicaid have to start using EVV by 2023. Some state governments use EVV technology too.

EVV technology can be in devices at home, apps on people's phones, or websites.

Wiley Reading is a white trans man. He has ADHD. Wiley is a PCA for a woman with cerebral palsy. They have to use EVV technology now.

But Wiley said the EVV technology is a nightmare. The EVV technology doesn't understand if two PCAs are there at the same time. The EVV technology also doesn't understand if PCAs have to do errands outside the house. And if Wiley makes a mistake, he has to fix it right away. If he doesn't fix it right away, he won't get paid. Even worse, sometimes the EVV technology makes mistakes on its own. When the EVV technology makes mistakes, Wiley loses pay too.

EVV technology invades disabled people's privacy. It can take over disabled people's lives.

EVV technology makes disabled people approve every little thing their PCAs do. They have to write down every time their PCA helps them use the toilet, clean something in the house, or take medications. They might have to do this lots of times every day. This is a lot of very personal information. It also takes a lot of time and attention to write it all down.

Some EVV technology uses cameras and microphones to watch disabled people and PCAs. Some EVV technology uses GPS systems that track people's exact locations. The federal government said GPS systems aren't required. But some EVV technology uses them anyway. And the GPS system can say a PCA has to stay inside a disabled person's house at work. This means disabled people can't go outside the house if they need support.

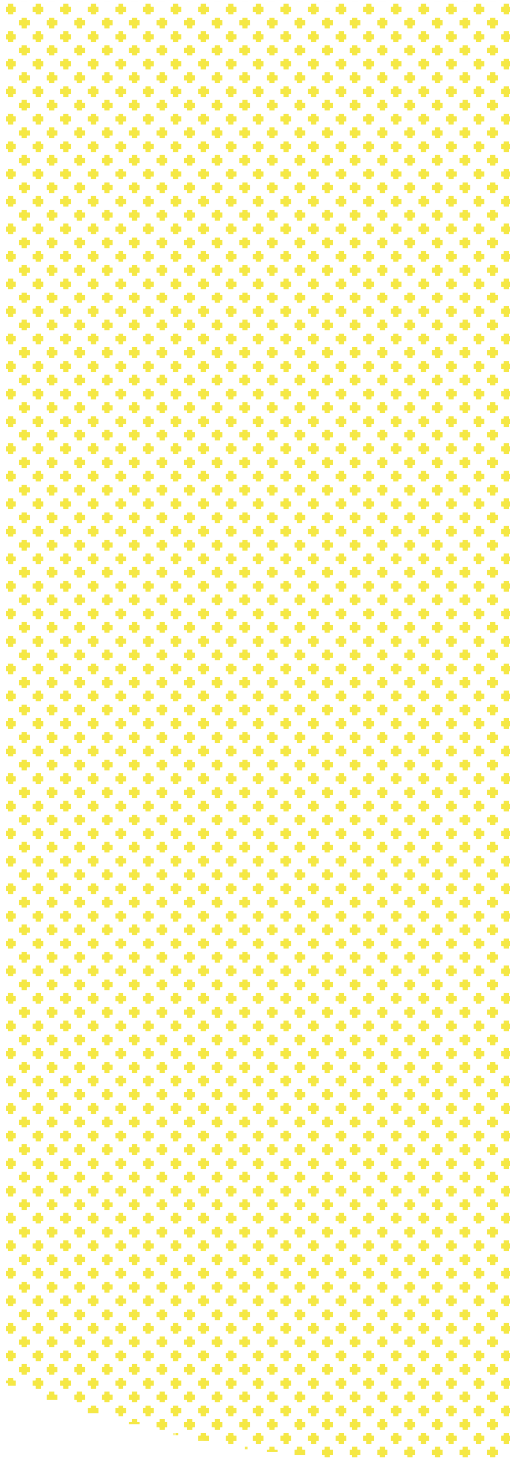
Advocates tried to make online forms to be easier for people with disabilities. But the federal government said the online forms weren't good enough. The government said they had to be a lot more detailed. That means people had to give up more privacy and control.

Forcing people to use invasive EVV is bad. Disabled people shouldn't have to choose between giving up privacy to stay at home, and going to an institution.

Recommendations:

- No one should use people's health information to discriminate.
- Tech companies and doctors should be very careful with people's health information. They should share as little information as possible. And they should make sure people can say no. People should have control over their information. People should get to decide who to share their information with.
- Researchers should ask permission before using people's social media posts. They should tell people what they want to do. They should give people regular reminders if they are using their information. And people should get to decide if they want to stop sharing. People should be able to ask researchers to delete their information too.
- State governments should tell people they don't have to use GPS tracking to follow the law. State governments should protect workers' privacy. State governments should also protect disabled people's privacy.

Surveillance at Work



Employers are using surveillance technology too. They watch what workers do. They decide if workers should get a raise or promotion. They decide if workers should get in trouble. And they try to get workers to do their jobs faster and better. Often, these technologies are very harmful.

One type of surveillance technology watches workers on the job. Another type of surveillance technology encourages people to get healthy. But both of these surveillance technologies can discriminate against disabled people. Disabled people deal with a lot of bias from coworkers and managers. Disabled people might get new injuries or illnesses at work. And companies might assume disabled people are unhealthy because they're disabled.

Algorithms that watch workers on the job

Lots of companies use hiring algorithms. These algorithms can discriminate against disabled people applying for jobs.

But companies use algorithms after they hire people too. Employers might use computer programs that spy on workers. They can watch workers through computer cameras. Employers might use algorithms to get workers to do their jobs faster. The algorithms can take away breaks and stop workers from resting. The algorithms can

punish workers for taking too many bathroom breaks or resting too much. The algorithms can automatically take away pay and even fire people.

Employers are watching workers on their phones and computers. Employers watch what workers do in a lot of types of jobs. They watch people working from home. They watch people who go to an office or job site. And they watch people who travel for work, like delivery workers.

Alma is an Asian American genderqueer person with multiple disabilities and chronic illnesses. They used to work in student support. Their supervisor used to spy on their computer calendar and online activity. Alma needs to take a lot of breaks. But their supervisor didn't like that. The supervisor started micromanaging every minute of Alma's work. The supervisor tracked every student Alma talked to. The supervisor tracked everything Alma talked about with students. The supervisor even tracked all the notes Alma took.

The supervisor wanted Alma to meet more students for less time. But Alma said that it was more important to take their time talking to students. Students agreed.

Algorithms that track workers can be dangerous for their health. They can make life worse for disabled people. And they can discriminate against disabled people too.

Making workers do their jobs faster is risky. Workers might get hurt in an accident. They could get hurt over and over again. And they could experience mental health effects from the pressure at work. The mental health effects can cause new disabilities too, like anxiety, depression, and trauma. And the algorithms can punish people for being disabled.

Disabled people often need more breaks. They need to rest. And they have to be flexible at work.

Disabled people are twice as likely to be jobless as nondisabled people. Disabled people working for low pay might stay in bad jobs. They might stay even if the job is dangerous and unfair. And disabled people of color deal with racism and ableism. So they might be worried about getting fired or discriminated against. And they might not speak up for themselves or advocate for their rights.

Algorithms at work might break the law. They might violate disability rights laws. And they might violate labor laws. Employers might violate the Americans with Disabilities Act if they automatically punish or fire people. Employers have to let people with disabilities ask for accommodations.

Nondisabled workers should be protected too. The Occupational Safety and Health Act (**OSHA**) says the government has to research worker safety. It also says the government has to make rules to protect workers. And it says employers have to follow the rules. Employers also have to protect workers from getting sick or hurt. The government hasn't talked about workplace algorithms. But the government has talked about workers getting hurt in the same ways workplace algorithms can hurt workers. So employers shouldn't use programs that can hurt workers.

Unfortunately, workers can't take their employers to court for health and safety issues. And the government doesn't have a lot of power to force employers to follow OSHA.

Company health and wellness programs

Some employers use algorithms that can hurt workers. But other employers use programs that try to encourage workers to be healthy. These programs offer rewards for participating. They reward workers for meeting goals about their weight, heart, walking, quitting smoking, or dieting. Some employers even punish workers for not participating. They might charge workers extra insurance payments.

These programs can discriminate against disabled workers. People with disabilities might not meet the expectations for being “healthy” based on nondisabled people. A lot of people assume being fat or disabled makes someone automatically unhealthy. But fat and disabled people can still be healthy.

In 2016, the U.S. Equal Employment Opportunity Commission said company health programs can’t ask for disability information. They also said employers have to offer rewards to nondisabled people and disabled people.

But disabled people might not have a fair chance. Disabled people might not be able to lower their blood pressure. Disabled people might not be able to walk a lot or at all. Disabled people might have trouble losing weight. So disabled people might not get to make a fair choice about company health programs.

Company health programs might not protect people’s privacy information. Companies might even share people’s information with other companies. Company health programs aren’t covered by an important health privacy law because they’re not a doctor’s office or insurance company. (That law is **HIPAA**, the Health Information Portability and Accountability Act.)

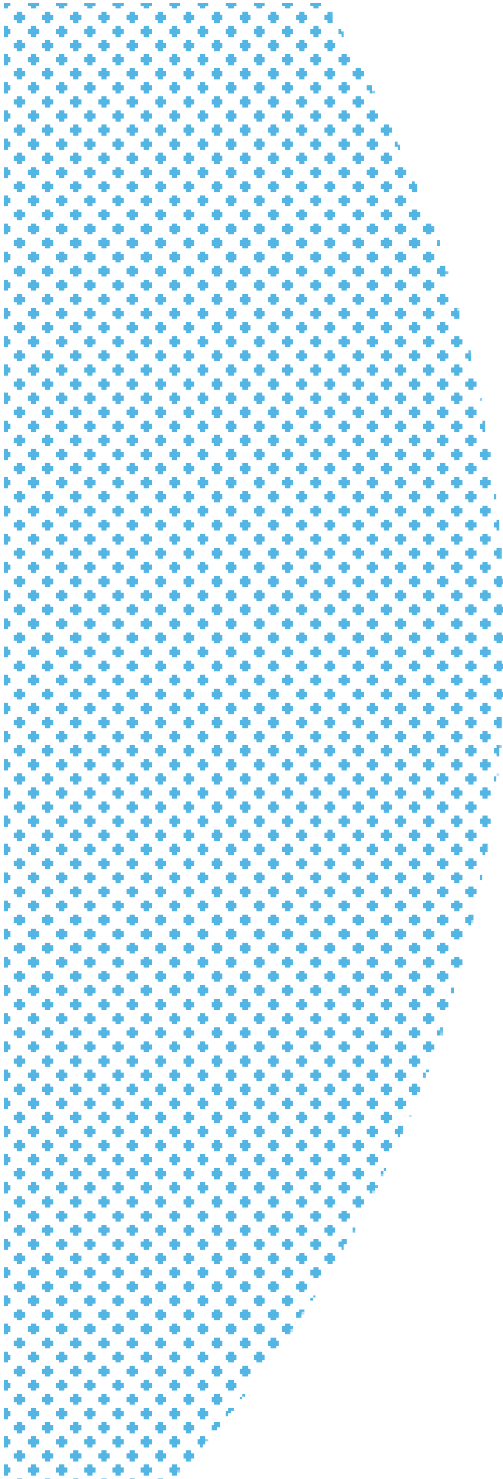
Houston, Texas made city workers share a lot of personal information. They had to share their entire disease history. They had to share if they ever used drugs. They had to share if they wore seat belts. And the health company said it might share this information with the public.

Sharing people’s health information at work is very dangerous.

Recommendations:

- Government agencies should tell employers they have to follow the law. Government agencies should tell company wellness programs they have to follow the law too. Workers should have a choice about joining a company wellness program. Employers shouldn't single out disabled people if they don't want to be.
- The government should do more research on how algorithms at work can hurt people. They should research how algorithms can be bad for mental health. They should research how algorithms can get people hurt or make people sick.
- The government should make employers stop using harmful algorithms.

Conclusion



Surveillance algorithms can discriminate against disabled people in lots of ways. Sometimes algorithms have good goals. They are supposed to stop cheating or violence. They are supposed to help people get healthy or do a good job at work. But algorithms can make bad decisions about disabled people's lives. Algorithms can discriminate against disabled people.

This report talked about how algorithms make life hard for disabled people. It talked about how algorithms don't understand disabled people. It talked about how algorithms work against disabled people.

But it doesn't have to be this way. We can make algorithms discriminate less. We can stop using algorithms that we know discriminate. Policy leaders, companies, and advocates can learn. We need to stop bad policies. Sometimes bad policies lead to harmful algorithms. If we stop the bad policies, then we can deal with algorithms that discriminate.

We shouldn't trust technology companies to check their own algorithms. Outside people need to double check if algorithms are biased.

Equality isn't the best goal either. If an algorithm causes people to unfairly lose their homes, it's bad

no matter who loses their homes. Algorithms should be fair in how they work. Algorithms should also be fair in what they do.

Policy leaders also need to protect people's privacy and information. They need to limit what companies and the government can do with people's information. They need to make rules about what information companies and the government can get. They need to make rules about who can use the information. They need to make rules about how long companies and the governments can keep the information.

Good policy comes from listening to people affected by it. It's about time governments and companies listened to disabled people.

Authors

Lydia X. Z. Brown is a policy counsel with CDT's Privacy & Data Project. They focus on disability rights and making algorithms fair and just. Their work has looked at algorithms that discriminate in public benefits, hiring, and surveillance. Lydia especially focuses on disabled people who are marginalized in more ways than one. Lydia also teaches part-time at Georgetown University. Their classes are about disability and gender.

Ridhi Shetty is a policy counsel with CDT's Privacy & Data Project. She focuses on equity (fair policies), privacy, and data. She also looks at how governments and companies use algorithms and AI.

Matthew U. Scherer is Senior Policy Counsel for Workers' Rights and Technology Policy. He works on AI, data, and other tech issues that affect workers.

Andrew Crawford is a Senior Policy Counsel with CDT's Privacy & Data Project. He focuses on protecting people's privacy related to their health. He works on how companies collect, share, and use health data.



cdt.org



cdt.org/contact



Center for Democracy &
Technology

1401 K Street NW, Suite 200



202-637-9800



@CenDemTech

