“Disability Discrimination and Automated Surveillance Technologies”

DATE
Thursday, August 25, 2022

FEATURING

Lydia X. Z. Brown
Policy Counsel, Privacy and Data Project, Center for Democracy & Technology

Ridhi Shetty
Policy Counsel, Privacy and Data Project, Center for Democracy & Technology

CSIS EXPERTS

Caitlin Chin
Fellow, Strategic Technologies Program, CSIS
Hello, welcome to the *This Does Not Compute* podcast series at CSIS. I’m your guest host, Caitlin Chin, taking over today for James Lewis. Today, I’m joined by Lydia X. Z. Brown and Ridhi Shetty, who are both policy counsels with the Privacy and Data project at the Center for Democracy and Technology, where they co-authored a recent report titled “Ableism and Disability Discrimination in New Surveillance Technologies.”

I’m looking forward to discussing some of the issues and findings from their research, but before we get started, I would love to do some quick introductions. First, Lydia and Ridhi, would you be able to give us an overview of your work at CDT? For example, what policy issues have you recently focused on, and what brought you to enter this space?

I can jump in first. My work focuses on how data-driven decision-making affects access to economic opportunity for marginalized communities and where the oversight and policymaking for these different practices tend to overlook intersections of marginalization. Our work focuses on particular areas of economic opportunity, ranging from employment to financial services to housing. And also corporate practices and how different regulatory bodies can be addressing each of these, both agencies that are tasked with particular areas of important anti-discrimination laws, like the EEOC and the Department of Housing and Urban Development, to agencies like the Federal Trade Commission that would be more targeted towards commercial entities like vendors.

This is Lydia X. Z. Brown, pronouns they/them. My work at CDT, similar to Ridhi’s, focuses on the social, economic, and political impact of algorithmic technologies—especially algorithmic bias and algorithmic discrimination and algorithmic harm on marginalized people. And particularly, my work focuses on algorithmic impacts on disabled people. Just to illustrate a little bit of what I mean by that, disability can cover a wide range of categories and experiences and identities. And so, algorithmic technologies can impact people with a wide range of manifestations of disabilities and different types of disabilities as well.

My work is focused on a number of ways in which algorithmic technologies mediate everyday life for disabled people, often with deeply critical implications for access to social services, economic participation and opportunity, civil and human rights—and just generally for our life, for our health, and for our freedom. Some of those issues have included algorithmic decision-making in public benefits determinations as well as employment processes, and in surveillance technologies that occur and are now ubiquitous in many parts of privately and publicly mediated life.

Thank you so much to you both for being here. It’s really important, when we talk about technology, to also recognize the people that it affects. Technology really does amplify existing societal problems. Things like ableism or access to public resources are not new challenges, but far too often our laws and policy frameworks don’t adequately prevent harm from surveillance or AI bias.

And with that, I’d like to dive right into your work in this area. Your research has called attention to where technology has presented outsized harms to disabled individuals, and I was wondering if you could illustrate some of the cases that
you've encountered in your research. In other words, where and in what contexts have you seen instances of biased AI either reinforcing ableism or failing to accommodate disabled people?

Ridhi Shetty: You can start by talking about how these technologies arise in the educational context. Schools monitor students both on and off school grounds through things like remote proctoring and using predictive analytics to detect threats to student safety and get their risks of dropout. Schools have relied a lot over the past couple of years, in particular during the pandemic, on automated virtual proctoring, which requires students to take exams in far more rigid settings than they would typically with human-driven proctoring. So, things like using scratch paper; taking breaks, or otherwise, stepping away from the screen, or stepping away from the laptop can be flagged as cheating. And these tools can end up penalizing students based on activity or needs that are related to disability.

These tools have also failed to recognize darker skin tones, which obligate students to direct bright lights at their test-taking space so the software will better detect their faces, which can trigger light sensitivity and pain, particularly for people who already have chronic pain or migraine or similar disabilities—and can also worsen anxiety, which will already be heightened during the test-taking period, and can be even worse for people who have mental health disabilities already.

There are also tools that schools are using for social media monitoring, for location tracking, facial recognition, aggression detection microphones, to determine whether a student is a threat to themselves or to others. And like automated proctoring, these tools can also misinterpret the data that they process, so they incorrectly flag students with certain disabilities as threats and even can disclose their disability status. These problems are even more acute for disabled Black and brown students and LGBT+ students. These tools are most likely to be used where the student population is predominantly Black and Latinx and to also surveil Muslim youth. And tools can out transgender students, expose students’ relationships, or their efforts to seek information pertaining to sexual or reproductive health or gender-affirming care.

And schools also use early dropout warning systems to detect students’ needs for academic support. These systems can consider things like attendance, academic performance, without also considering whether students previously lacked access or were denied access to necessary accommodations; whether they may have previously faced or currently face environmental and social barriers to their health; and other factors that could prevent academic success. These are just examples in the education context, but also then come up in the legal system, in healthcare, and in employment too.

Caitlin Chin: I was wondering what general trends you've been seeing in the use of technology in the education space. You mentioned COVID-19 and, as we know, the COVID-19 pandemic really did upend the world over the past couple of years. Many activities that might have otherwise been conducted in-person, such as taking exams, became remote. Now that more in-person activities are resuming, do you anticipate the trends that we've been seeing with remote proctoring, with schools monitoring social media, continuing?
This is Lydia. The acceleration of technologically-enabled surveillance certainly was not helped by the COVID-19 pandemic. But schools were already beginning to, at a very wide scale, deploy these kinds of technologies, especially—at least extensively—in the name of public safety. So, the examples that Ridhi was talking about—social media monitoring, facial recognition, aggression detection microphones, literal on-campus surveillance—as well as surveillance on school-issued devices, which some of our other colleagues at CDT have also recently published a report about.

These measures were already being undertaken by schools extensively to, number one, support students’ academic success, like Ridhi was just talking about. Number two, to protect students from fear of violent incidents within the school or from an outside-in shooter like through a mass shooting incident. And three, to promote the idea of school-wide integrity or community safety, but through imposing surveillance and functionally instituting a regime that’s based around tracking and potentially profiling and punishing students for not adhering to a norm for behavior, for dress code, for comportment, for appearance, for way of speaking, for way of inhabiting a body or physical space.

And really that’s why we’ve chosen to highlight the impact of surveillance tech on disabled people, because a lot of these technologies operate based on a presumption that there’s a correct or normal way for a person to function, for how their body or brain should operate, and if a student’s means of interfacing with test-taking software deviates from the norm, by definition, by design, the software will pick up on that deviation and assign it a level of suspicion for potential review, leading to possible disciplinary action and imposing a burden on a disabled person to either have to proactively disclose disability in the hopes that their disability will be accommodated—which is not a guarantee—or to have to prove, after the fact, that they were not in fact engaged in unethical behavior.

The aggression detection microphones example that we mentioned: there was a ProPublica investigation that we cite in our report that found that those microphones don’t have a very high accuracy rate and, in fact, have flagged as potential aggression or violence-indicating noises, innocuous sounds like a locker door slamming or really loud laughter. And people with a range of disabilities might make noises that fall outside that norm. It might be because of belonging to a specific cultural community where it’s more normalized to speak in louder, more externalized, emotive voices then in mainstream white culture and maybe because a disability, like cerebral palsy, or being hard of hearing, or being autistic, modulates somebody's voice volume. It may be because of a disability that affects mobility and dexterity. That means that a disabled person is more likely to slam objects just in order to physically use them or to drop things because of their disability.

So, in all of these examples that we’ve raised and talked about, the software itself operates to allegedly uphold some idea of what constitutes safety and academic integrity by further othering and profiling all those who deviate from the presumed norm.
Caitlin Chin: Now, from these examples that you're mentioning, I'm hearing several problems. First of all, the technology itself can be flawed. Like you mentioned with the example of aggression detection, there's a lack of accuracy when it comes to detecting voice volume, or perhaps exam proctoring algorithms have been trained to detect a certain manner of acting that does not apply to all individuals. But then there's also a second problem, which is that humans may apply technology or software in ways that are biased. So, I was just wondering what is your take; we know that AI and surveillance technologies can disproportionately hurt disabled people, but from your research, what have you found the root causes to be?

Lydia X. Z. Brown: This is Lydia. One of the most important phenomena that we need to name is the pervasiveness of ableism as a value system that assigns or removes value from people based on a range of actual or presumed characteristics, innate to our bodies and minds or external to them, based on how we are perceived or situated within our environments or communities. And those ableist values may manifest in assumptions about what it means to promote health, or what it means to be a productive and successful employee, or what it means to be considered a safe and non-threatening person in society.

Ridhi mentioned, just a couple of minutes ago, algorithmic technologies used to predict dropout rates or academic success. In one example that we mentioned in the report, the sheriff’s office in Broward County, Florida actually used data from the school district to flag youth as being at-risk for potential criminal activity based on a range of factors including receiving poor grades in school or lack of attendance in school. A person might receive poor grades or attend school less often for a wide range of reasons, including poverty, parental work schedules, their own caregiving responsibilities for younger siblings or more elderly or disabled family members, or because of their own disabilities that could cause a student to not be able to perform as well when they’re not receiving appropriate accommodations or support, or to not be able to attend school as frequently when expected to adhere to a certain schedule. And that creation of what sounds to me a lot like a real-life version of a pre-crime report—right, like channeling a certain blockbuster film here—is indicative of the ways in which ableist values shape our understanding of what constitutes a successful student, a safe non-criminal person, a productive industrious employee, or a healthy and well person. People who are affected in every single realm by algorithmic technologies.

So, if an algorithm is telling police where to allocate their resources and which people or neighborhoods to view with suspicion, or an algorithm is telling doctors and other clinical providers which patients might be non-compliant with medication and therefore require more stringent supervision, or literal surveillance methodologies—those algorithms are operated off of the same ableist values that inflict every aspect of society. The algorithms themselves reflect those ableist values and, in turn, reinforce those ableist values and impose them in the lives of all people who might be impacted by deployment of an algorithm—by their potential employer, their landlord, the police, their school, or any company that they might happen to interact with.

Caitlin Chin: That’s a really great way to put it—and that raises another question, and that’s the role of humans. Often when people talk about algorithmic bias or surveillance, I
hear human oversight proposed as a solution. But as we know, throughout history and like you mentioned, ableist values are unfortunately still ingrained in our society. Humans have implicit biases based on their experiences. So, I’m wondering, in many of the contexts that you’ve described, such as social media threat assessments or exam proctoring, would human oversight be an effective mechanism to prevent technology-enabled discrimination? In other words, could those discriminatory outcomes have been mitigated if a human decision-maker were present?

Ridhi Shetty: We often hear this argument that AI is going to inherently be less biased than humans will be, but algorithmic systems apply the standards that they were designed to apply so that they can perform the intended functions at scale. So, we need to think about where those standards come from and when we talk about human oversight, it should really be part of any algorithm-driven process. But to be clear, when we say human oversight, we don’t only mean a human is signing off on the ultimate decision that an algorithm influences. We also mean that the algorithmic tools must be examined, and their risks need to be corrected before the tools are deployed and even before the tools are procured, and we also mean that potential users of these tools should affirmatively decline to use these tools whose harms have been documented. For a lot of them, there’s been a lot of press coverage, a lot of studies done that document the inaccuracies of these tools, and yet they continue to use them anyway. So there needs to be accountability and responsibility for making that decision to adopt those tools regardless of previously documented risks.

We also mean that there needs to be ongoing review of how an already deployed tool may be creating new unanticipated risks for the populations on which it is used and what steps are being taken to address those risks. One challenge in examining how a tool can cause or exacerbate disability bias is that data on disability tends to be hard to come by. People often won’t disclose disability status for a few different reasons. One is the stigma that is attached to disability that causes people to basically be punished for being disabled. Another is that people don’t always know that they do in fact have disabilities, maybe because of cultural differences in how we talk about and understand disability or because of a lack of access to formal diagnosis, which tends to be a gatekeeper for obtaining any kind of supports and accommodations. And disability also isn’t easily measured because, as Lydia alluded to earlier, several factors will affect how the same disability presents and is experienced.

So, a more proactive examination of the risks of disability bias in a given tool is really important, and this includes scrutinizing the purpose for which the tool’s being used, how well it’s designed to fulfill that purpose, how it’s inputs might be proxies for protected traits, and how it’s outputs could affect disabled people, even if unintended. And a dialogue with and feedback from stakeholders about these factors is critical, particularly disabled experts who can recognize issues that people without disabilities may not even consider.

Lydia X. Z. Brown: This is Lydia. You know just building off of what Ridhi is saying, one of the issues about collection of disability data is that disabled people may also be understandably reluctant to share our data with researchers or advocates, let alone
Caitlin Chin: for-profit developers. Because we know in many marginalized communities, especially for those of us who are disabled—and also people of color, disabled, and part of the queer and trans communities—that when our data is collected at scale, it’s not always for benign purposes, and that the accuracy of an algorithmic tool doesn’t necessarily correlate to its morality or the morality of its usage.

For example, one of the algorithmic technologies that we’ve talked about quite a bit already today is surveillance technologies that might use facial recognition tech. And this conversation has come up a lot among advocates for racial equity and justice, that we know that facial recognition technology generally has tended to be less accurate for people of color and especially for women of color as compared to white men and white women. I’m not even including the experiences of transgender versus cisgender people, right? We know that around a range of axes of identity and experience, facial recognition technologies tend to be most accurate for cisgender white men—and less accurate for everybody else, particularly for Black women, for Asian women, and for non-binary and gender non-conforming people of all races.

Now we suspect, with rather limited data because there’s not been a lot of research on this, that facial recognition technologies are not necessarily accurate for disabled people in the same ways as for non-disabled people as well, and undoubtedly racial and gender differences would also apply to disabled people along those lines.

But many of us who are concerned about equity and justice and civil rights wonder what would happen if the algorithms were more accurate. It is a reflection of systematic bias and racism and sexism that facial recognition technologies have actually, in the last few years, allowed me to use my face to unlock another Asian’s phone. Like that’s a little bit problematic from a security perspective, from a user design perspective, that facial recognition for biometric access is touted as a more secure method of securing your accounts or your devices. But because the algorithm is based upon learning data, training data, that prioritizes white faces over East Asian faces, my face was able to bypass that security measure on another East Asian person’s phone. That’s not how it’s supposed to work.

But on the other hand, if police are using facial recognition technology, which we know they are, as those technologies become more accurate for people of marginalized communities, what does that say about the surveillance apparatus of the state and being able to more accurately identify political dissenters? And being able to accurately identify protesters who are exercising the right to peacefully protest? And being able to more accurately identify, profile, and criminalize people from marginalized communities who are already subjected to wide-scale societal biases and prejudices that make assumptions about our criminality and our suspicion because of race, color, religion, nationality, disability, and sexuality?

Caitlin Chin: Some of the cases that you’re describing are just so invasive and have so many implications for civil rights. Like you mentioned, for example, facial recognition in the context of policing or threat assessments. So my question is given all of these concerns, are facial recognition algorithms or predictive policing ever appropriate to conduct? Do you believe that, with proper safeguards, these risks to privacy or civil rights can be justified in some contexts? Or do you believe that there are other scenarios where predictive or automated tools should just be completely banned?
This is Ridhi. We have supported a moratorium on law enforcement use of facial recognition technologies until strong, effective, robust protections are established for its use, and we’ve also supported a ban on automated proctoring programs. Ideally, any use of algorithmic or data-driven tools that affect the areas that we’re talking about today—whether you’re talking about law enforcement, education, employment, or the healthcare system—they should all be used to expand access to these opportunities and these supports.

But, at the very least, entities should be proactively examining and mitigating—if not eliminating—the discriminatory impact of the tools that they choose to adopt. So, if the risks and the harms that are posed by a new resource can’t be remedied, then that tool should no longer be used.

You mentioned that CDT has supported a moratorium on facial recognition in the context of policing until strong, effective, robust protections are adopted—what might those look like?

A lot of it would be examining the impacts that the tool’s going to have before its being deployed. A lot of the tools that we see being used in the law enforcement context range from predictive policing systems to risk assessment tools to, being more specific, gunshot detection, where these technologies have been documented to be either inaccurate or to increase policing for particular neighborhoods and particular communities.

So these tools, especially when it’s known that they pose particularly disproportionate impacts for certain communities, before they can be adopted there has to be a review process and, especially when you’re talking about tools that government entities are going to be implementing, should also be subject to public input as well. There should be a comment period for people to be able to talk about how their particular communities have been affected by similar technologies in the past. So, these really need to be policy decisions that are made with meaningful community input before they can be adopted.

And specifically, input from the communities that have the most to lose. The ones who already have been, and will continue to be, the most impacted by discriminatory, prejudiced values, policies, and practices.

Absolutely, I 100 percent agree with that. Now I am curious, in your view, who would be responsible for implementing these reviews or these safeguards? For example, should the entity that deploys algorithms such as schools, or government entities, or other businesses, be in charge of auditing their outcomes? Or do you believe AI developers should be in charge of preventing bias? Or is it both?

Well, I’ll give employment as an example. On one hand, you have the employers who are opting to adopt these technologies and often really heavily relying on the information and promises they get from vendors. Under federal anti-discrimination laws, employment agencies are also covered entities. When talking about employment discrimination, there are often debates around whether vendors also should be considered employment agencies, even though they are increasingly
performing the functions that any employment agency would be performing. We would argue that they should be liable as employment agencies under federal anti-discrimination law.

So, it should be this multi-stakeholder approach. Employers need to be responsible for the tools that they adopt before and during their adoption. Vendors need to be responsible, especially when you see vendors making promises of their tools being less biased or having been examined for bias when they haven't really been examined sufficiently for disability bias, or even sufficiently examined for other forms of bias either:

And there also needs to be an ongoing dialogue between community and regulators as well. We’re really heartened to see the EEOC’s attention to AI’s impacts, especially when it comes to tools that are being used in the hiring context. They recently issued guidance back in May, but we hope going forward to see more guidance that also addresses the intersections of how these tools will affect disabled people who are multiply-marginalized as well.

Caitlin Chin: You mentioned existing federal laws that relate to disability or other types of discrimination, and I was wondering if you could just give us an overview of these. Could you talk about how the current legal framework applies to AI and surveillance and do you believe that existing statutes are enough to prevent disability discrimination?

Ridhi Shetty: One example, of course, is the Americans with Disabilities Act (ADA), which prohibits employment practices that treat employees adversely based on their disabilities and fail to provide reasonable accommodations when doing so would not pose an undue hardship on employers. The ADA and the Rehabilitation Act also prohibit entities that receive federal funding from denying someone the benefits of their funded programs based on the person’s disability. Then there’s also the Occupational Safety and Health Act which requires employers to provide safe and healthy workplaces.

And so, a lot of tools that are used for instance in the employment context, like algorithmic management tools that monitor productivity and performance tracking, may prevent workers from taking breaks and can increase physical injury and also have some negative mental health impacts. These kinds of tools could violate the ADA.

The problem is that algorithmic and other data-driven systems have become an instrumentality for discrimination. They allow public and private sector entities to disguise their discriminatory behavior with these seemingly neutral systems. Which is why we rarely see disability discrimination claims regarding these systems. People don't really have access to how their information is being used and what data precisely is being gathered, how it’s going to be evaluated, and how that’s going to render an adverse decision. That information asymmetry, information gap, is really a big barrier to ensuring thorough enforcement of these laws.

There’s also the Fair Credit Reporting Act, particularly relevant in things like the housing context when you’re talking about how tenant screening algorithms and
facial recognition, other surveillance technologies, are used by landlords. The Fair Credit Reporting Act requires accuracy of information in consumer reports, which includes info bearing on credit worthiness, character reputation, personal characteristics, mode of living. These factors can be proxies for disability and they can be informed by consumers’ online activity, social networks, communications, location data, employment and education history, and purchase and payment history.

The companies that collect and share this data often claim that they’re not consumer reporting agencies so the Fair Credit Reporting Act wouldn’t apply to them. And that’s particularly concerning when you think about the other kinds of technologies—for instance, in the criminal legal system, and how data that’s collected in the housing context then bleeds into the criminal legal system too. So, if somebody has had evictions in the past, regardless of the reason why they had a history of eviction, that can contribute to an arrest record. The Department of Housing and Urban Development has even advised against using criminal history that does not indicate history of conviction. They’ve advised against using that kind of data to make these decisions, and yet they are continuing to be used to deny housing and other related opportunities and to further criminalize people.

So, even though these laws exist, the enforcement tends to be muddied by the role that these particular third parties, essentially, have in the relationship between the consumer and the person on whom decisions are being made and the user of that tool. That developer or vendor tends to be in a gray area.

Caitlin Chin: So, I understand that there had been some gray areas when it comes to either the applicability of current laws or their enforcement. But I was wondering, have we seen any legal challenges so far related to how new technologies can impact discrimination in the disability context—and, if so, what were those outcomes?

Ridhi Shetty: I don’t think that we’ve seen claims on the basis of disability in particular, because it can be particularly hard to gather information that indicates that the discrimination was on the basis of disability specifically. If we think about how, for instance in the criminal legal system, often symptoms of mental health disability will be mistaken or interpreted as aggression, or a propensity for violence, so those are both racially coded and also just general stereotypes when it comes to how attributes that are relevant to disability are really attributed to character traits or personality traits. Those things can make it more difficult to ensure that those people who are being penalized by these technologies can recognize that disability’s really the basis on which they’ve been discriminated—so to trace that down the line, and to be able to indicate that this is the result of disability discrimination, in particular, is more difficult.

Same thing with, for instance, the employment context. Say we were encountering a performance monitoring tool that was detecting how we talk to people—it can perform sentiment analysis with your customer service conversations, things like that—if the tool is collecting information about your tone of voice, how you’ve been talking, your word choice, those can be relevant to disability but it may not be clear that’s what you’re being penalized on the basis of. It’s harder to tie that to disability as the actual grounds for the discriminatory action. It can be challenging to be able
to pinpoint the actual basis for which somebody has been penalized for a certain tool and that just makes it harder to be able to pursue this kind of claim.

And at the same time, we also have the fact that not everybody even is aware that they could pursue a disability claim, whether it’s because they’re not aware that they have a disability or because they’re afraid to disclose that to the people who would be responsible for enforcement.

Caitlin Chin: That’s right, the system shouldn’t put the onus on people to prevent discrimination. That responsibility needs to lie on the entities or the individuals that use the algorithms or potentially perpetuate discrimination themselves.

Throughout this conversation, we’ve talked about discrimination in very high-impact contexts; for example, we’ve talked about law enforcement, education, employment, and healthcare. But, in your view, should context matter when we talk about protections from discrimination and disparate treatment? For example, what about something like targeted advertising based on disability or race? How should policymakers and companies be thinking about that?

Ridhi Shetty: Well, I can jump in to start. One thing that you need to be thinking about is the purpose for which any of these different tools are being used and what kind of values are driving their use.

For instance, in the targeted advertising space, a lot of it is about messaging, like which audience you want to reach, which audience you’re valuing, and then which kind of messages are being interpreted for what they are versus being subject to stereotypes. For instance, there was a case some time ago about an advertisement for adaptive clothing on Facebook. That advertisement was taken down because it violated Facebook’s policy, even though not only was there nothing inappropriate about the clothing being advertised, but it was specifically geared towards the disability community. And in those cases, the algorithm isn’t taking into account who that ad is intended to serve beyond these more defined categories of interest areas and affinity groups.

So in those situations, the context that we’re talking about is really whether that algorithm is able to parse through who’s going to value this content and why, and also be able to make a reliable judgment about what kind of harms, if any, are being caused.

Caitlin Chin: That’s a very good example of how targeted advertising can pose harms, and I completely agree it’s a question of the ableist values that Lydia mentioned earlier but also access to information more broadly. So I agree that targeted advertising shouldn’t escape notice either.

Ridhi and Lydia, thank you so much for this conversation and for sharing your expertise with us. One of my biggest takeaways is that disability discrimination is not only an AI issue, but it’s also a privacy issue and a surveillance issue and a civil rights issue. So, I do have one more question for both of you: can commercial privacy protections affect some of the issues that we’ve discussed today? We’ve talked a little bit about safeguards for AI or civil rights, but just as some background
for our listeners, right now Congress is considering federal comprehensive privacy legislation such as the American Data Privacy and Protection Act that would ban companies from collecting or processing personal information in a manner that discriminates based on disability. And it would also open the door for external researchers or auditors to conduct impact assessments on how large companies mitigate discrimination in certain contexts. And that’s just one example of a bill, but I would really love to hear your perspectives on whether or not privacy protections can impact ableism and disability discrimination in general.

Ridhi Shetty: I think it absolutely could make a huge difference for, particularly, the risks that data collection can pose for disabled people. Often, marginalized communities are put in a position where they have to choose between either protecting their data or accessing supports or any kind of technologies that would enable independent living or enable access to information, access to communications. And so, by ensuring that there are really meaningful privacy protections in terms of minimizing the data that’s collected and stored and shared in the first place, ensuring that technologies are being scrutinized before and during their use—that’s really critical for disabled people.

You have a range of different technologies that could be particularly risky. Some include, for instance, devices that are used at home just to do simple things like managing or using your appliances, turning your lights on and off, adjusting your home temperature, to using social media. That range of different ways in which your data can be exploited and misused and shared can be particularly harmful for disabled people. Another recent example was there was one company that provides this nonprofit mental health support service that was collecting data and then sharing it with its for-profit spin-off to train customer service technologies—and that’s a use of personal data, very sensitive data, that is not only exploitative, but it’s just not what you expect when you are turning to a certain kind of technology at a very vulnerable moment for support.

There are certain kinds of technologies, certain kinds of data, that should really just be off limits to that kind of data sharing, and really robust privacy protections can ensure that data is not being shared beyond what is necessary in order to provide the service that the person is expecting to receive and has really signed up for.

Caitlin Chin: That’s right, as a basic principle companies shouldn’t use personal information in ways that harm people. And I’m with you, I do believe that it’s very hard to solve some of the tech- or data-related discrimination issues that we’ve observed without basic boundaries on how companies collect and process personal information.

So, I’ll definitely keep my eye on privacy and surveillance developments and whether we’ll see those potential benefits play out. Once again, our guest speakers today are Lydia X. Z. Brown and Ridhi Shetty of the Center for Democracy and Technology. I highly encourage all of our listeners to check out their work on AI bias, surveillance, and disability discrimination on the CDT website. And to Lydia and Ridhi, thank you so much again for all of your work on these crucial issues and for joining us today.

Ridhi Shetty: Thank you so much Caitlin, really glad to talk.
Lydia X. Z. Brown: Thank you so much for having us.