NEW AMERICA

March 2021

Working and Learning During the Pandemic

Surveillance of Students and Employees is Not the Cure

Koustubh “K.J.” Bagchi, Christine Bannan, & Raj Gambhir

Acknowledgments

The authors would like to thank Representative Anna Eshoo, Sarah David Heydemann, Wilnieda Negrón, Anisha Reddy, and Kent Wada for participating in the event highlighted in this report along with Austin Adams and Lisa Johnson for communications support. Open Technology Institute would also like to thank Craig Newmark Philanthropies for generously supporting our work in this area. The views expressed in this report are those of its authors and do not necessarily represent the views of Craig Newmark Philanthropies, its officers, or its employees.

About the Author(s)

Koustubh "K.J." Bagchi is senior policy counsel at New America's Open Technology Institute, focusing on platform accountability and privacy issues.

Christine Bannan is policy counsel at New America's Open Technology Institute, focusing on platform accountability and privacy.

Raj Gambhir is a Legal/Public Policy intern with New America's Open Technology Institute, working with the platform accountability and privacy teams.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Introduction

More than half a million lives have been lost to COVID-19 in the United States since the disease was first identified over a year ago.[1] While vaccine distribution has increased across the country in the past few months, no one knows when the pandemic will end.[2] Society has had to adapt over the past year, and standard education and workplace practices have shifted dramatically. Schools and workplaces operating in person, remotely, or both have had to find ways to safeguard the health of students and workers while successfully continuing operations. Under these circumstances, schools and employers have looked to, and continue to use, technological tools like exam-proctoring software and wearables.

Unfortunately, tools for monitoring student and employee behavior, both in person and remotely, are often deployed without meaningful safeguards to protect against privacy and equity threats to students and employees. Further, how institutions handle feedback to the deployment of these tools has also come under scrutiny. In response to equity, privacy, and civil liberties concerns around the use of such tools as segments of American society were reopened, Members of Congress introduced three bills in 2020.[3] New America's Open Technology Institute (OTI) supported the introduction of two of them: the Public Health Emergency Privacy Act[4] and the Exposure Notification Privacy Act.[5] Additionally, OTI also co-led the development of principles with 83 civil rights, civil liberties, labor, and consumer protection organizations that are designed to guide decisions about whether and when the use of such technologies is appropriate.[6]

This report builds on an event OTI held on October 15, 2020 that specifically explored technological tools deployed in the workplace and school environments to both ensure that individuals are not exposed to COVID-19 and monitor the productivity of students and employees.[7] Moderated by OTI policy counsel Christine Bannan, this panel included Sarah David Heydemann, Senior Counsel for Education and Workplace Justice at National Women's Law Center; Wilneida Negrón, Director of Policy & Research at Coworker.org; Anisha Reddy, Youth & Education Privacy Policy Counsel at Future of Privacy Forum; and Kent Wada, Chief Privacy Officer and Director of Policy and Governance at UCLA. The panel addressed the following questions: Are surveillance tools being deployed during the pandemic effective and appropriate responses to limiting the spread of COVID-19? What guardrails can and should be put in place to protect student and employee rights, along with their health?

Following the panel discussion, U.S. Rep. Anna Eshoo (D-Calif.), Chair of the House Energy and Commerce Committee's Subcommittee on Health, discussed her bill, the Public Health Emergency Privacy Act.[8]

Health and Safety Measures

Schools and workplaces across the country have instituted new health and safety monitoring tools for the stated purpose of allowing operations to continue or resume while minimizing COVID-19 infection. Though it has been over a year since this pandemic began, it is still not clear to what extent these tools serve their purpose.[9] Furthermore, many employers and school administrators are continuing to wrestle with the question of how to implement these tools in a privacy-protecting manner.

Though there have been a variety of health monitoring tools deployed, we will focus on two prominent tools that our panelists discussed: thermal imaging systems and health monitoring wearables. After describing each tool, we will provide an account of how relevant stakeholders—including the affected students and workers as well as experts in various fields—have responded to the tool's rollout. Finally, we will detail how the schools and workplaces deploying these tools have responded to stakeholder feedback.

Thermal Imaging Systems

Based on early guidance from the Centers for Disease Control (CDC), schools and employers commonly consider high fever to be a major symptom of COVID-19.[10] Many schools[11] and workplaces[12] use mandatory temperature checks as a health and safety measure for those working or studying in person. In order to avoid possible viral transmission when taking temperatures, the Food and Drug Administration (FDA) recommends the use of contactless thermometers.[13] There are two main types of contactless thermometers: thermometer guns used to manually take temperature from a short distance,[14] and thermal imaging cameras which use infrared sensing, sometimes paired with facial recognition, to automatically measure the temperature of anyone in range.[15]

Vendors have begun to offer contactless thermometers to schools and businesses across the country as a response to the onset and continuation of the COVID-19 pandemic. For example, a number of Subway restaurants in Southern California [16] and colleges across the country[17] have implemented PopID kiosks. Originally designed to use facial recognition to allow employees into their workplace and let customers pay with their face, the kiosks can now be retrofitted with a thermal camera, allowing the kiosk to measure employee and student temperature automatically.[18] Video technology company OneScreen offers a similar facial recognition-based security and temperature measurement system that has been installed in schools from New York to California.[19]

Despite the popularity of thermal imaging technologies as a pandemic-related health measure, public health and privacy experts have criticized the accuracy of these technologies and the utility of relying on fever as an indicator of COVID-19 infection. According to more current guidance from the CDC, the prevalence of asymptomatic or mild cases among those who can nevertheless spread the virus makes mandatory temperature checks insufficient health and safety measures on their own.[20] Additionally, privacy experts argue that thermal imaging systems not only have dubious public health value, but also erode civil liberties by normalizing persistent and invasive surveillance, especially in the case of thermal imaging systems equipped with facial recognition.[21] As opposed to thermometer guns, thermal imaging cameras capture much more than temperature, tracking individuals' movements, and in some cases biometric identifiers.[22]

Workers themselves subjected to this invasive technology have pushed back. Last fall, former Amazon employee Michael Jerinic sued Amazon under the Illinois Biometric Information Privacy Act (BIPA) for allegedly collecting employee biometric data without soliciting consent during mandatory thermal imaging temperature checks.[23] Amazon has not publicly responded to the allegations of BIPA violations made by Jerinic.

Additionally, some school administrators and education privacy experts have expressed concern over the use of thermal imaging, including Catherine Cullen. Cullen, a school board member of Rio Rancho Public Schools in New Mexico, voted against a measure to acquire OneScreen thermal imaging kiosks for the district, citing civil liberties and data governance concerns.[24] Ultimately, Rio Rancho Public Schools voted to purchase OneScreen tablets, but resolved not to use the kiosks' facial recognition capabilities.[25]

Other education experts are urging schools to be cognizant of the inaccuracy of thermal imaging systems. During the panel, Anisha Reddy, Youth & Education Privacy Policy Counsel at Future of Privacy Forum, recommended that school districts not turn students away from school solely on the basis of a temperature check. "A temperature check may not be super accurate, so there should be another human level of a decision-making process before a student is turned away from school," she urged.

Wearables for Health Monitoring

Some schools[26] and workplaces[27] have responded to the challenges of the pandemic by making health monitoring wearables a mandatory or optional part of in-person operations. This section will focus on the deployment of wearables in schools and workplaces for the purposes of location-tracking and symptom monitoring.[28]

In the context of the pandemic, wearables that track the location of students and workers have been deployed for two interrelated purposes. The first is to aid in contact tracing, or the tracking of who an infected person may have come into contact with and thereby infected.[29] Some firms have built their own in-house contact tracing applications that they market to other companies. For example, the consultancy firm PwC's contact tracing suite, Check-In, uses either a mobile app or a wearable device to collect proximity data from employees. Once an employee reports themselves as ill, an administrator can see at a glance who the worker has come into contact with and can then begin notifying these individuals of their possible exposure.[30] When PwC reopened its first office last spring in Shanghai, the company required that all returning workers use Check-In,[31] and as of August of last year has planned to make the use of Check-In mandatory at all PwC offices in the United States.[32]

The second purpose of deploying location-tracking wearables in schools and workplaces is to enforce social distancing guidelines. Wearable devices like the TraceTag affix to a worker's hardhat or are worn on the body. If workers contravene social distancing guidelines by standing too close to each other, the TraceTag sets off an audible alarm and begins to flash, warning the worker to step back. A number of such wearable devices, the TraceTag included, also serve as passive location trackers in order to facilitate contact tracing.[33] Gilbane Building Company, one of the largest construction companies in the United States,[34] has issued TraceTags to all carpenters at a number of its job sites, utilizing the tool to enforce social distancing guidelines and conduct contact tracing.[35]

Along with deploying wearable devices for location tracking purposes, some schools and workplaces are utilizing wearable devices to monitor COVID-19 symptoms. Detroit's Oakland University has been using the BioButton, a coin-sized device worn on the skin that continuously monitors vital signs and temperature, to conduct student symptom monitoring.[36] That data is uploaded to a dashboard, where administrators in schools or workplaces can track symptoms of potential infections.[37] Like the TraceTag, the BioButton has the secondary purpose of facilitating contact tracing.[38]

Expert opinion on the use of wearable health trackers as a means to limit COVID-19 infection is mixed. Ethics experts like those at the Harvard Safra Center argue that the proliferation and enforced use of wearable health monitors could normalize public and private surveillance of the body, paving the way for location tracking long after the threat of COVID-19 abates.[39] Far from denying this possibility, some vendors have leaned into it, making it a selling point. Airista Flow, a vendor of wearable trackers, has published a blog post detailing possible post-pandemic use cases of their tracking tags, including ensuring "people/assets stay within (or outside of) predefined boundaries."[40]

Some students and workers subject to these technologies have pushed back. As part of its reopening plan for Fall 2020, Detroit's Oakland University had planned to make it mandatory for students returning to campus to wear the BioButton.[41] In response, a senior at the university started a petition asking the university to make the wearing of the BioButton optional due to the technology posing a "large overreach in terms of student and staff privacy."[42] The petition quickly garnered thousands of signatures, and within a week Oakland University acceded to its demand.[43]

Among medical experts opinions on the use of wearables as a means of pandemic response tend toward cautious and qualified approval. Dr. Amesh Adalja of the Johns Hopkins Center for Health Security suggests that, if combined with a genuine institutional concern for safety and an otherwise robust pandemic response plan, wearables can serve as a useful pandemic response tool.[44] Other medical experts argue for more transparency with health monitoring wearables, with one research paper proposing that such wearables include labels that enumerate appropriate use cases and clearly convey the measurement accuracy of said wearables.[45] Still others view the proliferation of health monitoring wearables during the pandemic as an opportunity to collect large volumes of data that could train machine learning algorithms to detect asymptomatic cases of COVID-19.[46]

Wilneida Negrón, a panelist and director of Policy & Research at Coworker.org, suggested that employees who find that wearables are entering their workplace learn from athletes, who have long had to deal with wearable technology and ensure that their data is protected from abuse. "People that are in the athletic field or sports have had to wear wearables historically for many years. . . And so looking at how those athletes have been able to create that governing structure and that collective bargaining agreement is a period of learning. What is language and what other sectors can we learn from?" Education privacy experts can also learn from these data governance agreements in service of addressing the rollout of wearable technologies in schools.

At some workplaces that have deployed health-monitoring wearables, there have been rumblings of discontent. In June of last year, it became publicly known that Amazon was testing the use of wearables that emit a sound if workers stand in close proximity.[47] Amazon warehouse workers, who had not been informed of these tests, expressed disapproval at the possibility of these wearables being implemented, with some noting that warehouse working conditions make the six-foot distance requirement impossible.[48] Whether this discontent fizzles away as wearables become more common, boils over into widespread and open opposition, or is resolved through negotiation and legislation, is yet to be seen.

Performance and Productivity Monitoring

Employers and school administrators have turned to new tools during the pandemic to monitor the work and learning of workers and students. Although some schools and employers used productivity monitoring tools before COVID-19, the pandemic has made these tools more widespread.[49] Workers are facing different levels and types of surveillance depending on whether their job is white-collar or blue-collar. Wilneida Negrón explained during our panel, "We're seeing a segmentation of the workplace, the labor market in terms of essential workers, those workers that are working from home which are much more professional, and then you have the unemployed. And each of those types of workers are experiencing a different type of technology." Further, workers in low-wage jobs have been subject to the most extensive surveillance both before[50] and during the pandemic.[51] As explained by Sarah David Heydemann, senior counsel for Education and Workplace Justice at National Women's Law Center, during our panel, "We see the effects of these privacy violations playing out even more harshly on communities that have traditionally been marginalized in different ways in the workforce."

Employers who originally present tools to workers as health measures may also use the tools to monitor worker productivity. Marketing material for workplace wearables tends to blur the line between the tools' public health and productivity functions.[52] As explained by Negrón during our panel, "We've been noticing for over five years the increasing use of workforce management surveillance technologies. What we're seeing now is not only an increased safety need, but also the sophistication of these new technologies."

The pandemic has accelerated the use of surveillance technologies in both K-12 and higher education settings, and across different industries. This section will focus on two technologies that experienced rapid expansion since March of 2020: exam proctoring software and device monitoring software. Each discussion will begin by explaining the motivations universities and employers have for using these tools, describe the response from students and workers, and examine how criticism was received by school administrations, workplaces, and vendors. It will conclude by making recommendations to schools and workplaces.

Exam Proctoring Software

The transition to remote learning has increased concerns about academic integrity, which schools have tried to address using exam proctoring software. There are many vendors providing proctoring services to academic institutions at all levels, including Proctorio,[53] ProctorU,[54] Honorlock,[55] Examity,[56] and Respondus.[57] The pandemic has accelerated demand for proctoring services: In

May of 2020, Proctorio reported that business had increased 900 percent after campuses began closing.[58] During the panel, Chief Privacy Officer and Director of Policy and Governance at UCLA Kent Wada expressed the concerns of professors and administrators: "There's been a huge spike over the last several months in academic dishonesty cases. . . how do you deal with this? Integrity is such a cornerstone [of the university]." According to ProctorU data, rates of cheating on the exams that it proctored increased approximately eight-fold with the onset of the pandemic,[59] and the vendors' assertions that cheating has become more common have further increased the demand for their services.[60] While it is clear that virtual learning increases the challenges of proctoring exams to ensure academic integrity, critics have questioned the reliability of the methods used to detect cheating.

The proctoring software many universities use relies on a combination of facial recognition and eye-movement tracking that poses privacy and equity threats. The technology has disparate impacts on students of color and students with disabilities. Studies show that facial recognition technology is significantly less accurate for people of color, and its use in school proctoring software has created difficulties for students with darker skin. Honorlock, a popular exam proctoring service, is powered by Amazon's controversial AI facial recognition system Rekognition.[61] In June of 2020, Amazon announced a one-year moratorium[62] on police use of Rekognition due to studies showing it misidentified people of color at higher rates than white people,[63] but has not stopped its use in education.

The risks of inaccuracy are greater in the law enforcement context where systems seek to identify an unknown individual with a one-to-many match, than in the one-to-one matching context of verifying that a particular exam-taker is the correct person. However, there are nonetheless multiple examples of inaccuracy in the exam proctoring context that are posing serious obstacles to students in online-only environments. Most proctoring software verifies that the correct person is sitting for an exam by using facial recognition to match the student's face with their photo ID, and failure to match can prevent students from taking exams or require students to take exams under uncomfortable conditions. For example, a Black student had to shine a bright light on her face throughout an entire exam so the software could recognize her[64] and an Arab-American law graduate tried 75 times to verify his identity but the bar exam software could not recognize him.[65] As Anisha Reddy noted during our panel, "It's unacceptable for a tool that requires video to recognize a student's face to not recognize a Black student's face, because these decisions that these tools can make are really going to impact a student's future."

Proctoring software has also been found to erroneously flag neuro-atypical and disabled students for cheating because of their irregular eye movements or hyperactivity.[66] The programs assume that students who move often are looking away from the screen to read prohibited materials.[67] A test-taker's suspicion level

is calculated by whether the movements taken during an exam fall outside the standard deviation.[68] Students with autism or other neuro-atypical attributes, visual impairments, neuromuscular disorders, or any medical reason requiring administering medication or using the restroom frequently during exams all fall outside the standard deviation, and are flagged by algorithmic systems.[69] Kent Wada underscored the importance of focusing on the disparate impacts of privacy violations on marginalized groups during our panel, "When you think about privacy, there's a really big area of exploration that we can still look forward to at the intersection of equity and inclusion, particularly and certainly diversity."

Students have protested the use of exam proctoring software for a number of reasons, including the technology's disparate impacts on students of color and students with disabilities, accessibility issues for students with unreliable internet access, and the stressful environment created by surveillance.[70] Many have taken collective action to petition school administrators for more equitable learning conditions, collecting signatures and writing open letters.[71] Searches for Proctorio, ProctorU, HonorLock, and other exam-proctoring companies on Change.org will return dozens of petitions organized by students opposing their school's use of the software.[72]

Some college administrations have been responsive to student concerns about the privacy and equity problems created by exam proctoring software. After students at the City University of New York collected over 28,000 signatures[73] petitioning the administration to stop using Proctortrack, the university announced it would change its plans to use methods of assessment that did not require the software.[74] Further, the University of California, Berkeley prohibited instructors from using online proctoring services because the administration was "unable to find a viable option that would address student privacy concerns and accommodations."[75]

However, some vendors have retaliated against students and staff who criticize their exam proctoring software. After a computer science student criticized Proctorio on Twitter and posted an analysis of its code on Pastebin, the company banned his IP address and the CEO sent him a message threatening legal action if he did not remove his posts.[76] Additionally, ProctorU threatened to sue faculty members at the University of California, Santa Barbara who sent a letter to the administration raising concerns with the company's data-sharing practices and asking the university to terminate its contract with the company.[77] Finally, Proctorio sued a university staff member after he posted links to videos that the company showed instructors to draw public attention to the company's practices.[78]

Device Monitoring

Just as the shift to remote education has caused greater concern about academic integrity, the shift to remote work has caused concerns about worker productivity, leading some employers to turn to monitoring technology. Early in the pandemic, surveys found that 40 percent of managers expressed low confidence in their ability to remotely manage their workers[79] and 78 percent of business leaders believed that the shift to hybrid or remote work would negatively impact worker productivity.[80] However, evidence of remote work's impact on productivity is varied and context-dependent.[81] One study found an increase in productivity for knowledge workers who began working remotely during the pandemic,[82] but another study found a precipitous drop in productivity with the transition to remote work.[83] The global demand for employee monitoring software increased by 87 percent in April 2020.[84] The rush to adapt to the pandemic in 2020 has caused some employers to overlook privacy and security issues with remote monitoring tools. According to the International Association of Privacy Professionals, about 60 percent of employers that have adopted new technology during the pandemic have expedited or skipped entirely privacy and security reviews.[85]

Many employers have required remote workers to install activity-tracking software that uses keystroke loggers, cameras, and screen sharing.[86] These vendors include StaffCop,[87] Teramind,[88] Hubstaff,[89] CleverControl,[90] and Time Doctor.[91] Hubstaff gives workers "productivity scores" in 10-minute increments based on the percentage of time spent typing.[92] Other software takes periodic screenshots and photos of employees to send to their managers.[93]

Unsurprisingly, these surveillance tools are generally not popular with employees [94] because they violate privacy and exacerbate challenges caused by the pandemic. The monitoring of remote workers has disproportionately impacted people with childcare responsibilities, including helping children with remote learning, who are more likely to be women.[95] During our panel, Sarah David Heydemann noted that, "Reddit is full of work-from-home hacks for seeming like you're still online … How [else] are you going to take breaks to breastfeed? How are you supposed to be watching your children that have their school lessons to attend to and show the same level of productivity? Oftentimes it just isn't possible."[96] Heydemann noted the findings of a National Women's Law Center Study: "There were more than 1.1 million workers who were forced out of the labor force as a result of the pandemic and a full 80 percent of those were women.[97] Working women and Latinas were especially overrepresented in that number." Working parents, particularly mothers, have needed extra support to manage childcare during the pandemic to sustain productivity, but instead many employers have tried to use surveillance.

Recommendations for Schools and Workplaces

The COVID-19 pandemic has placed many schools and workplaces in the difficult position of finding ways to resume or continue operations while protecting both the health and privacy of students and workers. The following recommendations can mitigate some of the concerns raised by privacy experts.

1) School administrators should consider less invasive alternatives to surveillance technologies.

Before employers and schools implement any monitoring technologies, they should ensure that the technology is needed to serve a valid safety, productivity, or integrity purpose. This means that employers and schools should both determine whether the purpose to which they may deploy the tool in question is valid, and decide whether the tool itself is truly needed for that purpose.

For example, in many circumstances proctoring surveillance tools may not be necessary because there are alternative methods to assess student performance that are equally or more effective. Universities that have decided not to use exam proctoring software have created policies and implemented solutions to help instructors protect both privacy and academic integrity.[99] Alternatives to the use of proctoring software like open book exams, student-developed quiz questions, and group projects[100] demonstrate that in many cases, valid health and productivity concerns caused by the pandemic can be addressed with privacy-respecting and relatively equitable solutions.

2) Before purchasing a surveillance technology, school administrators and employers should determine that technology's efficacy.

Schools and workplaces should ensure that the surveillance tools they are interested in implementing serve their purported health or productivity monitoring functions. As OTI noted in a 2020 white paper on contact tracing, institutions should avoid adopting or continuing use of surveillance tools that collect data that is "neither useful nor appropriate" for the purposes they intend to serve.[101] In the context of pandemic-related response in schools and workplaces, this means making an informed judgement about whether or not tools actually protect health or increase productivity.

Unfortunately, some schools[102] and workplaces[103] adopted health and productivity monitoring tools without proper vetting. During our panel, Wilneida Negrón explained, "There's just an influx of new tools and technologies that are not being vetted. We don't know if they're doing what they're intended to be doing and [they] could be sowing the seeds of a continuing hyper-vigilant workplace."

As detailed in the Health and Safety Measures section of this report, public health authorities and healthcare providers have been gradually sounding the alarm about the insufficiency of temperature checks as a response to the pandemic given the prevalence of asymptomatic COVID-19 cases.[104] Under these circumstances, the health and safety purpose of mass temperature checks on their own does not appear to be valid, and thus the acquisition of thermal imaging systems without more fundamental measures, such as guaranteed sick leave and access to testing also appears invalid.

Moreover, the equity problems with technology can also create accuracy and efficacy issues. When exam proctoring software misidentifies the behavior of disabled students as suspicious,[105] that tech is not only inequitable, but also inaccurate, because it delivers false positives.

3) School administrators and workers should practice transparency and incorporate stakeholder feedback,

Schools and workplaces should solicit and take into account the input of relevant stakeholders when implementing new health and safety technologies.[106] At a minimum, students and workers should be informed of what health monitoring tools are being introduced, aware of how the data collected by those tools would be used, and have an active decision-making role in whether and how these tools are deployed and utilized.

As explained by Kent Wada during our panel, "It's not like we can control everything, but disclosing what we can and can't control, what we do and don't do [means that while] people may not agree with our position, at least then they're focusing on the real issues as opposed to just speculating." Similarly, as articulated during our panel by Anisha Reddy, "With regard to proctoring, I think a huge thing is that there should be opportunities for students to communicate issues that they're experiencing to their teachers and institutions and to feel heard, that these issues are being considered and there should be alternatives available to students."

Many activity monitoring tools allow employers to decide whether or not to make their workers aware that they are being monitored and intentionally make their software difficult to detect.[107] Secretly installing software to monitor workers covertly is never appropriate. When an employer finds it necessary to use activity monitoring technology, workers must be informed both what specific tool is used and the types of data it collects.

4) School administrators and employers should consult with privacy experts and conduct impact assessments.

In addition to directly consulting with those being required to use health or productivity monitoring tools during the pandemic, workplaces and schools deploying these tools should familiarize themselves with the numerous best

practices documents drafted by privacy experts,[108] and directly consult with privacy experts, implementing the best practices offered by privacy experts to the greatest extent possible.

Schools and workplaces introducing new surveillance tools in response to the COVID-19 pandemic could also conduct privacy impact assessments (PIAs) to understand the effect that these tools have on their students and workers respectively, and take steps to mitigate the privacy risks. PIAs are a legal requirement for Federal government agencies developing or procuring certain types of information technology systems.[109] For instance, to document the privacy impact of its own contact tracing system, NASA released a PIA that detailed the system's categories of data collected, consent mechanism, security controls, information sharing practices, redress mechanisms, and compliance with existing laws.[110] If schools and workplaces conduct PIAs before deciding whether to use a tool or enter a contract with a vendor, they will be better positioned to make informed decisions.

Schools and workplaces should also assess whether tools could have a disparate impact on students and workers belonging to marginalized populations. Algorithmic impact assessments can "assess the short and long term impacts of these systems, whose interests they serve, and if they are sufficiently sophisticated to contend with complex social and historical contexts."[111] This type of analysis could help employers and school administrators identify methods to mitigate any disparate impact or determine that the risks posed by a tool outweigh its benefits.

5) School administrators and employers should minimize the data collected by surveillance technologies.

As OTI has urged in regard to higher education online learning,[112] institutions utilizing data collection tools in response to the pandemic must minimize the volume and categories of data collected to only those needed for specific, clearly articulated purposes. This means collecting the minimum amount of data needed to implement legitimate workplace and schoolplace safety and monitoring measures. For example, instead of using exam proctoring software that continuously collects biometric information, schools could choose alternative models that capture images of students screens during exams.[113] This approach could minimize the amounts and types of sensitive data collected while fulfilling the objective of academic integrity.

Sarah David Heydemann asserted during our panel that is the responsibility of employers to be, "ensuring that the data that's collected is for a particular purpose that doesn't go beyond the bounds of what's necessary, that there's an understanding of how long it will be kept for, and frankly an understanding of what kind of profit is being made off of the data that workers are, perhaps, unwillingly or unwittingly providing."

6) Surveillance technologies deployed in the school and workplace should only be used for narrow and explicitly defined purposes.

Data collected for the purpose of maintaining the health and safety of workers and students during this pandemic must be only used for that purpose. This means that the use of all health and safety surveillance tools deployed in response to the pandemic must end once the pandemic ends, and the data collected by those tools must not be used for unrelated purposes.[114] As explained by Anisha Reddy during our panel, "There should be a clearly defined purpose for this new data that's being collected to ensure it's only being used for that specific purpose and not being repurposed later on."

Recommendations for Policymakers

Policymakers must also consider a number of recommendations to curb any abuse of these technological tools. Action on the part of receptive employers and school administrators to ensure accountability for the tools deployed to guarantee the health, safety, and productivity of their respective employees and students is insufficient to protect their privacy and safety without concerted government action.

1) Congress must pass comprehensive privacy legislation.

A comprehensive privacy law would be the most important step policymakers can take to ensure protections around data use, access, and storage practices as it relates to technological tools utilized by private companies during the pandemic.[115] Among other provisions, Congress should codify requirements that companies follow privacy best practices such as those outlined above as recommended voluntary measures. A comprehensive data privacy law would also limit the data handling practices of companies that provide tech tools to public schools and universities. Further, through a comprehensive privacy law, Congress could establish transparency requirements to provide greater accountability. Creating a consistent set of standards for how industry players treat personal data would also be a major step towards mitigating harms and minimizing potential abuse of that data. Such a law could also inspire confidence in students and employees about the tools being deployed on them.

2) Federal and state policymakers should enhance education privacy protections.

While worker privacy would be bolstered by federal comprehensive privacy legislation, lawmakers seeking to protect student privacy need to pursue more targeted interventions. Fortunately, there are a number of actionable steps that lawmakers can take to protect student privacy during this pandemic. One measure that may be effective is updating the Family Educational Rights and Privacy Act (FERPA),[116] the primary law protecting student privacy. FERPA regulates the disclosure of students' personally identifiable information (PII) which includes direct identifiers, like students' names, and indirect identifiers, such as date of birth, which can allow re-identification through combination with other data points.[117] Given the increasing use of education technology over the past few years,[118] the volume of data collected about students has increased substantially,[119] leading some lawmakers to call for reforming FERPA. In 2014, Sens. Ed Markey (D-Mass.) and Orrin Hatch (R-Utah) introduced a FERPA reform bill that would have put data minimization, deletion, and data security measures requirements on student data held by third parties.[120] Restarting the conversation around updating FERPA would be a fruitful step in protecting student privacy during the pandemic and beyond.

In addition, the Department of Education (ED) could issue further guidance to schools on how to respect student privacy during the COVID-19 pandemic and beyond, as we face a potential future of increased use of remote learning technologies. In March 2020, ED put out guidance instructing school administrators and public health officials on how to navigate FERPA requirements during the pandemic.[121] That same month, ED held a webinar on how FERPA applies to online learning, running participants through scenarios regarding PII disclosure during online learning.[122] ED could bolster these efforts by holding more webinars and issuing further guidance, focusing on issues of education technology vetting and procurement during the pandemic.

Further, local and state lawmakers could pursue legislative reform to further student privacy. One instance of recent legislative reform on the issue of student privacy is New York State's December 2020 law which imposes a moratorium on the use of biometric technology in schools, and mandates a study examining the use of these technologies.[123] Given the novelty and disparate impact of biometric tools such as facial recognition,[124] this measure benefits student privacy and should be emulated by other state legislatures.

3) In the short term, Congress should pass narrower legislation that focuses on privacy rights as it pertains to combating the spread of COVID-19.

In the short term, policymakers could consider legislation that has a narrower focus on technological tools deployed to combat COVID-19. For example, Rep. Eshoo, who spoke at OTI's event, co-sponsored legislation, the Public Health Emergency Privacy Act, that applies to all digital tools used in a pandemic response. Specifically, the bill includes a data minimization provision stating that an organization should only collect data when "necessary, proportionate, and limited for a good faith public health purpose."

As Rep. Anna Eshoo explained at the event, "What I thought then as I do now is that we need balance. We should use technologies that can help save lives and reduce the spread of COVID-19. That's a human effort. And that is essential. But the data that is collected by these technologies, whether they're controlled by the government or private companies should not be used for any other use, only for public health."

Conclusion

The rapid onset of the pandemic forced schools and workplaces to make difficult choices about the institution of healthy, safety, and productivity measures, choices that should be revisited and reconsidered if warranted. As Kent Wada articulated during our panel, "We know that and so our actions today really do make a difference for the future. And again we have to acknowledge that emergencies require emergency responses, but where we can we need to take that step back."

As the pandemic stretches on, the continuation of education and employment opportunities is central to re-establishing the major pillars of our functioning society. While the use of some technological tools deployed in response to the pandemic can have beneficial effects, employers and schools should adhere to important privacy-protective principles, and policymakers should establish needed guardrails to ensure that we protect both the safety and the privacy of employees and students.

Notes

1 "COVID-19 United States Cases by County," Johns Hopkins University, Feb. 23, 2021, https://coronavirus.jhu.edu/us-map

2 "Covid-19: The World Has Changed. So Has the Playbook for the Olympics.," New York Times, Feb. 15, 2021, https://www.nytimes.com/live/2021/02/03/world/covid-19-coronavirus

3 "Congress Considers Three Bills Addressing Privacy Protections During COVID-19 Crisis," New America, July 14, 2020, https://www.newamerica.org/oti/blog/congress-considers-three-bills-addressing-privacy-protections-during-covid-19-crisis/

4 "S.3749 - Public Health Emergency Privacy Act," Congress.gov, May 14, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3749

5 "S.3861 - Exposure Notification Privacy Act," Congress.gov, Jun. 1, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3861

6 "Civil Rights Groups Call for Protection of Democracy and Privacy as Tech Responds to Pandemic," New America, June 11, 2020, https://www.newamerica.org/oti/press-releases/civil-rights-groups-call-protection-democracy-and-privacy-tech-responds-pandemic/

7 "[ONLINE] - Working and Learning During the Pandemic: Surveillance of Students and Employees is Not the Cure," New America, Oct. 15, 2020, https://www.newamerica.org/oti/events/working-and-learning-during-pandemic/

8 "H.R.6866 - Public Health Emergency Privacy Act," Congress.gov, May 14, 2020, https://www.congress.gov/bill/116th-congress/house-bill/6866

9 "Infrared Fever Detectors Used for COVID-19 Aren't As Accurate As You Think," IEEE Spectrum, Dec. 11, 2020, https://spectrum.ieee.org/news-from-around-ieee/the-institute/ieee-member-news/infrared-fever-detectors-used-for-covid19-arent-as-accurate-as-you-think

10 "Interim Clinical Guidance for Management of Patients with Confirmed 2019 Novel Coronavirus (2019-nCoV) Infection," Internet Archive Wayback Machine, Jan. 30, 2020, https://web.archive.org/web/20200201032438/cdc.gov/coronavirus/2019-ncov/hcp/clinical-guidance-management-patients.html

11 "Schools Are Doing COVID-19 Temperature Checks: Do They Really Help?," Education Week, Nov. 10, 2020, https://www.edweek.org/leadership/schools-are-doing-covid-19-temperature-checks-do-they-really-help/2020/11

12 "Facial recognition temperature scanning, wearables and voice biometrics deployed for COVID-19 spread prevention," Biometric Update, Aug. 3, 2020, https://www.biometricupdate.com/202008/facial-recognition-temperature-scanning-wearables-and-voice-biometrics-deployed-for-covid-19-spread-prevention

13 "Non-contact Temperature Assessment Devices During the COVID-19 Pandemic," FDA, June 19, 2020, https://www.fda.gov/medical-devices/coronavirus-covid-19-and-medical-devices/non-contact-temperature-assessment-devices-during-covid-19-pandemic

14 "Non-contact Infrared Thermometers," FDA, May 23, 2020, https://www.fda.gov/medical-devices/general-hospital-devices-and-supplies/non-contact-infrared-thermometers

15 "Thermal Imaging Systems (Infrared Thermographic Systems / Thermal Imaging Cameras)," FDA, Jan. 11, 2021, https://www.fda.gov/medical-devices/general-hospital-devices-and-

supplies/thermal-imaging-systems-infrared-thermographic-systems-thermal-imaging-cameras

16 "Employers Rush to Adopt Virus Screening. The Tools May Not Help Much.," New York Times, May 14, 2020, https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html

17 "University of Mississippi deploys PopID automated temperature testing," Kiosk Marketplace, Aug. 28, 2020, https://www.kioskmarketplace.com/news/university-of-mississippi-deploys-popid-automated-temperature-testing/

18 "Secure, contact-free building access using facial recognition," PopID, Feb. 23, 2021, https://www.popid.com/entry

19 "How Schools and Businesses Are Reopening Using New Tech: GoSafe in the News," OneScreen Solutions, Sep. 19, 2020, https://www.onescreensolutions.com/en/blog/how-schools-and-businesses-are-reopening-using-new-tech-gosafe-in-the-news/35060052689

20 "FAQs for Workplaces & Businesses," CDC, Feb. 11, 2021, https://www.cdc.gov/coronavirus/2019-ncov/community/general-business-faq.html

21 "Temperature Screening and Civil Liberties During an Epidemic," ACLU, May 19, 2020, https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_temperature_checks.pdf

22 "Research shows gains in biometric identification from thermal images as contracts increase," Biometric Update, Jan. 15, 2020, https://www.biometricupdate.com/202001/research-shows-gains-in-biometric-identification-from-thermal-images-as-contracts-increase

23 "Amazon COVID-19 Scans Ignore Workers' Rights, Ill. Suit Says," Law360, Oct. 8, 2020, https://www.law360.com/articles/1318190/amazon-covid-19-scans-ignore-workers-rights-ill-suit-says

24 "Schools Adopt Face Recognition in the Name of Fighting Covid," Wired, Nov. 03, 2020, https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid/

25 "Schools Adopt Face Recognition in the Name of Fighting Covid," Wired, Nov. 03, 2020, https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid/

26 "Reopening Schools Issue Brief: Wearable Technologies & COVID-19," Student Privacy Compass, Aug. 3, 2020, https://studentprivacycompass.org/reopening-3/

27 "Back to Work: Wearables Track Social Distancing and Sick Employees in the Workplace," IEEE Spectrum, May 1, 2020, https://spectrum.ieee.org/the-human-os/biomedical/devices/wearables-track-social-distancing-sick-employees-workplace

28 "Wearables and the Internet of Things for Health," Research Gate, Sep. 27, 2016, https://www.researchgate.net/profile/Michael_Schwartz31/publication/309853585_Wearables_and_the_Internet_of_Things_for_Health_Wearable_Interconnected_Devices_Promise_More_Efficient_and_Comprehensive_Health_Care/links/5ec3fb0aa6fdcc90d685abf2/Wearables-and-the-Internet-of-Things-for-Health-Wearable-Interconnected-Devices-Promise-More-Efficient-and-Comprehensive-Health-Care.pdf

29 "Contact tracing and COVID-19: What is it and how does it work?," Mayo Clinic, Dec. 15, 2020, https://www.mayoclinic.org/diseases-conditions/coronavirus/expert-answers/covid-19-contact-tracing/faq-20488330

30 "Check-In: A PwC Product," PwC, Feb. 23, 2021, https://www.pwc.com/us/en/products/check-in.html

31 "Your Boss May Soon Track You At Work For Coronavirus Safety," NPR, May 8, 2020, https://

www.npr.org/2020/05/08/852896051/your-boss-may-soon-track-you-at-work-for-coronavirus-safety

32 "Scared of going back to the office? Companies hope these apps will help," CNN Business, Aug. 20, 2020, https://www.cnn.com/2020/08/19/tech/back-to-office-business-covid-apps/index.html

33 "In the Time of COVID-19 – How Will You Maintain Safe Working Distances?," Triax, Feb. 23, 2020, https://www.triaxtec.com/social-distancing-contact-tracing/

34 "ENR 2020 Top 400 Contractors," Engineering News-Record, Feb, 23, 2021, https://www.enr.com/toplists/2020-Top-400-Contractors-Preview

35 "Union Carpenters Utilizing New Technology to Better Social Distancing," Eastern Atlantic States: Regional Council of Carpenters, May 28, 2020, https://eascarpenters.org/union-carpenters-utilizing-new-technology-to-better-social-distancing/

36 "Wearable BioButton now available to campus community," Oakland University News, Nov. 19, 2020, https://oakland.edu/oumagazine/news/campus-community/2020/wearable-biobutton-now-available-to-campus-community-

37 "NEW! BioButton™ COVID-19 Screening Solution," BioIntelliSense, Feb. 23, 2021, https://biointellisense.com/biobutton

38 "Website, Application, and Product User Terms of Use," BioIntelliSense, Oct. 2020, https://biointellisense.com/legal/website-and-product-user-terms-of-use

39 "Ethical Implementation of Wearables in Pandemic Response: A Call for a Paradigm Shift," Edmond J. Safra Center, May 18, 2020, https://ethics.harvard.edu/files/center-for-ethics/files/18ethicalwearables.pdf

40 "POST-COVID USE CASES: YOU HAVE THE TAGS, LET'S PUT THEM TO OTHER USES!," Airista Flow, Oct. 9, 2020, https://blog.airistaflow.com/blog/post-covid-use-cases-0

41 "The Hot New Covid Tech Is Wearable and Constantly Tracks You," New York Times, Nov. 15, 2020, https://www.nytimes.com/2020/11/15/technology/virus-wearable-tracker-privacy.html

42 "Make the BioButton Optional for Staff and Students at Oakland University," Change.org, Aug. 3, 2020, https://www.change.org/p/oakland-university-make-the-biobutton-optional-for-staff-and-students-at-oakland-university

43 "BioButtons become optional after public outcry," The Oakland Post, Aug. 7, 2020, https://oaklandpostonline.com/32739/campus/biobuttons-become-optional-after-public-outcry/

44 "University walks back mandatory health tracking devices for students to control COVID-19, but experts say it could have been a 'good thing'," Yahoo! Life, Aug. 3, 2020, https://www.yahoo.com/lifestyle/university-walks-back-mandatory-health-tracking-devices-students-control-coronavirus-spread-211500160.html

45 "Wearables in the SARS-CoV-2 Pandemic: What Are They Good for?," JMIR Publications, Dec. 22, 2020, https://mhealth.jmir.org/2020/12/e25137

46 Continuous on-body sensing for the COVID-19 pandemic: Gaps and opportunities," ScienceAdvances, Sep. 2, 2020, https://advances.sciencemag.org/content/6/36/eabd4794?utm_campaign=toc_advances_2020-09-04&et_rid=689771818&et_cid=3471286

47 "Amazon is testing a wearable device that lights up and beeps when warehouse workers get too close to each other," CNBC, Jun. 16, 2020, https://www.cnbc.com/2020/06/16/amazon-tests-wearable-social-distancing-device-for-warehouse-workers.html

48 "Amazon faces backlash over Covid-19 safety measures," BBC, June 17, 2020, https://www.bbc.com/news/technology-53079624

49 "The Workplace-Surveillance Technology Boom", Slate, May 12, 2020, https://slate.com/technology/2020/05/workplace-surveillance-apps-coronavirus.html

50 "The psychosocial impacts of technological change in contemporary workplaces, and trade union responses," International Labor Organization, 2016, https://labordoc.ilo.org/discovery/delivery/41ILO_INST:41ILO_V2/1271828430002676?lang=en

51 "COVID-19, the gig economy and the hunger for surveillance," Ada Lovelace Institute, Dec. 8, 2020, https://www.adalovelaceinstitute.org/blog/covid-19-gig-economy-hunger-for-surveillance/

52 "3 Covid-19 Workplace Concerns Wearable Tech Addresses," Wear Kinetic, June 25, 2020, https://www.wearkinetic.com/3-covid-19-workplace-concerns-wearable-tech-addresses/

53 "Not just proctoring. A Comprehensive Learning Integrity Platform.," Proctorio, Feb. 23, 2021, https://proctorio.com/

54 "Exam Security. Done Right.," ProctorU, Feb. 23, 2021, https://www.proctoru.com

55 "Online Exam Proctoring with a Human Touch," Honorlock, Feb. 23, 2021, https://honorlock.com/

56 "Online proctoring, on your terms," Examity, Feb. 23, 2021, https://www.examity.com/

57 "Who We Are," Respondus, Feb. 23, 2021, https://web.respondus.com/

58 "Keeping Online Testing Honest? Or an Orwellian Overreach?," New York Times, May 10, 2020, https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html

59 "Online cheating surges during the pandemic; universities struggle to find a solution," San Francisco Chronicle, Nov. 6, 2020, https://www.sfchronicle.com/education/article/Online-cheating-surges-during-the-pandemic-15696066.php

60 "Colleges flock to online proctors, but equity concerns remain", Higher Ed Dive, Apr. 7, 2020, https://www.educationdive.com/news/colleges-flock-to-online-proctors-but-equity-concerns-remain/575642/

61 "Online Proctoring Renaissance Powered by Artificial Intelligence and Machine Learning," AWS Startups Blog, Nov. 9, 2020, https://aws.amazon.com/blogs/startups/online-proctoring-renaissance-powered-by-ai-and-ml/

62 "We are implementing a one-year moratorium on police use of Rekognition," About Amazon, June 10, 2020, https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition?ots=1&tag=w050b-20&linkCode=w50

63 "Amazon Won't Let Police Use Its Facial-Recognition Tech for One Year," Wired, June 10, 2020, https://www.wired.com/story/amazon-facial-recognition-police-one-year-ban-rekognition/

64 "Software that monitors students during tests perpetuates inequality and violates their privacy," MIT Technology Review, Aug. 7, 2020, https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/

65 "Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools," Vice Motherboard, Sep. 24, 2020, https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools

66 "Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education," Hybrid Pedagogy, Apr. 2, 2020, https://hybridpedagogy.org/our-bodies-

encoded-algorithmic-test-proctoring-in-higher-education/

67 "Exam Security. Done Right.," ProctorU, Feb. 23, 2021, https://www.proctoru.com

68 "Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools," Vice Motherboard, Sep. 24, 2020, https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools

69 "Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education," Hybrid Pedagogy, Apr. 2, 2020, https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/

70 "Cheating-detection companies made millions during the pandemic. Now students are fighting back.," The Washington Post, Nov. 12, 2020, https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/

71 "Students Are Pushing Back Against Proctoring Surveillance Apps," EFF, Sep. 25, 2020, https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps

72 "SEARCH: proctoru," Change.org, Feb. 23, 2021, https://www.change.org/search?q=proctoru

73 "Do Not Let CUNY Violate Student Privacy," Change.org, Oct. 22, 2020, https://www.change.org/p/chancellor-f%C3%A9lix-v-matos-rodr%C3%ADguez-do-not-let-cuny-violate-student-privacy

74 "Victory: University will not proceed with the implementation of Proctortrack," Change.org, Oct. 22, 2020, https://www.change.org/p/chancellor-f%C3%A9lix-v-matos-rodr%C3%ADguez-do-not-let-cuny-violate-student-privacy/u/27937419

75 "Guidance and Recommendations for Instructors and Students on Proctoring and Final Examinations," UC
Berkeley Academic Senate, Apr. 20, 2020, https://academic-senate.berkeley.edu/sites/default/files/guidance_and_recommendations_from_the_working_group_on_exams_and_proctoring.pdf

76 "Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools," Vice Motherboard, Sep. 24, 2020, https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools

77 "Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools," Vice Motherboard, Sep. 24, 2020, https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools

78 "An ed-tech specialist spoke out about remote testing software — and now he's being sued," The Verge, Oct. 22, 2020, https://www.theverge.com/2020/10/22/21526792/proctorio-online-test-proctoring-lawsuit-universities-students-coronavirus

79 "Remote Managers Are Having Trust Issues," Harvard Business Review, July 30, 2020, https://hbr.org/2020/07/remote-managers-are-having-trust-issues

80 "The Future of Jobs Report: 2020, World Economic Forum, Oct. 2020, http://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf

81 "The Influence of Working from Home on Employees' Productivity," Stockholm School of Economics, 2020, https://www.diva-portal.org/smash/get/diva2:1446903/FULLTEXT01.pdf

82 "Research: Knowledge Workers Are More Productive from Home," Harvard Business Review, Aug. 31, 2020, https://hbr.org/2020/08/research-knowledge-workers-are-more-productive-from-home

83 "Co-workers working from home and individual and team performance," National Library of

Medicine, Mar. 2020, https://pubmed.ncbi.nlm.nih.gov/32214593/

84 "Employee Surveillance Software Demand up 51% Since Start of Pandemic," Top 10 VPN, Nov. 18, 2020, https://www.top10vpn.com/research/investigations/covid-employee-surveillance/

85 "PRIVACY IN THE WAKE OF COVID-19," IAPP, May 2020, https://iapp.org/media/pdf/resource_center/iapp_ey_privacy_in_wake_of_covid_19_report.pdf#page=31

86 "Your Boss Is Watching You: Work-From-Home Boom Leads To More Surveillance," NPR, May 13, 2020, https://www.npr.org/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance

87 "StaffCop Enterprise: Employee Monitoring & Threat Detection Software," StaffCop, Feb. 23, 2021, https://www.staffcop.com/

88 "User Activity Monitoring + Data Loss Prevention + User Behavior Analytics = Teramind," Teramind, Feb. 23, 2021, https://www.teramind.co/

89 "Time tracking. Reporting. Peace of mind.," Hubstaff, Feb. 23, 2021, https://hubstaff.com/

90 "TOTAL CONTROL OVER EMPLOYEES' COMPUTERS. MONITOR FROM ANYWHERE AROUND THE WORLD. QUICK INSTALLATION IN 2 CLICKS!," CleverCONTROL, Feb. 23, 2021, https://clevercontrol.com/

91 "Time tracking software to help your team be more productive while working from home," Time Doctor, Feb. 23, 2021, https://www.timedoctor.com

92 "How My Boss Monitors Me While I Work From Home," New York Times, May 6, 2020, https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html

93 "Your Boss Is Watching You: Work-From-Home Boom Leads To More Surveillance," NPR, May 13, 2020, https://www.npr.org/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance

94 "Workers are not prepared for the future of working from home," Prospect, Oct. 2, 2020, https://prospect.org.uk/news/workers-are-not-prepared-for-the-future-of-working-from-home/

95 "Working Moms Bear Brunt of Home Schooling While Working During COVID-19," United States Census Bureau, Aug. 18, 2020, https://www.census.gov/library/stories/2020/08/parents-juggle-work-and-child-care-during-pandemic.html

96 "ULPT: Need to cheat on a proctored, online exam? Make a cheat sheet and put it on your laptop screen.," Reddit, 2020, https://www.reddit.com/r/UnethicalLifeProTips/comments/ckf3fu/ulpt_need_to_cheat_on_a_proctored_online_exam/

97 "Four Times More Women Than Men Dropped Out of the Labor Force in September," National Women's Law Center, Oct. 2, 2020, https://nwlc.org/resources/four-times-more-women-than-men-dropped-out-of-the-labor-force-in-september/

98 "A Gendered Pandemic: Childcare, Homeschooling, and Parents' Employment During COVID-19," SocArXiv, Feb. 10, 2021, https://osf.io/preprints/socarxiv/gwkzx/

99 "Guidance and Recommendations for Instructors and Students on Proctoring and Final Examinations," UC
Berkeley Academic Senate, Apr. 20, 2020, https://academic-senate.berkeley.edu/sites/default/files/guidance_and_recommendations_from_the_working_group_on_exams_and_proctoring.pdf

100 "Alternatives to Proctored Exams," Kentucky Community & Technical College Systems, Feb. 23, 2021, https://kctcs.edu/education-training/kctcs-

online/learn-by-term/proctor-exams/alternatives-to-proctored-exams.aspx

101 "Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns," Edmond J. Safra Center and New America Open Technology Institute (OTI), May 18, 2020, https://newamericadotorg.s3.amazonaws.com/documents/Safra-OTI-NA_Contact_Tracing_Paper.pdf

102 "Massive Shift to Remote Learning Prompts Big Data Privacy Concerns," Education Week, Mar. 27, 2020, https://www.edweek.org/technology/massive-shift-to-remote-learning-prompts-big-data-privacy-concerns/2020/03

103 "PRIVACY IN THE WAKE OF COVID-19, PART 2," IAPP, Jan. 2021, https://iapp.org/media/pdf/resource_center/iapp_ey_privacy_in_wake_of_covid_19_report_part2.pdf#page=8

104 "Do temperature checks help screen for COVID-19? Doctors say checking for fever alone isn't enough," 4WWL, Aug. 19, 2020, https://www.wwltv.com/article/news/health/coronavirus/health-experts-say-temperature-screenings-are-not-enough-for-virus-detection-in-public-places/289-5ba773ec-3c67-4b1a-aa1e-b026d62efd5b

105 "How Automated Test Proctoring Software Discriminates Against Disabled Students," Center for Democracy and Technology, Nov. 16, 2020, https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/

106 "Virtual Classrooms and Real Harms," arXiv, Dec. 10, 2020, https://arxiv.org/pdf/2012.05867.pdf

107 "Inside the Invasive, Secretive "Bossware" Tracking Workers," EFF, June 30, 2020, https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers

108 "Civil Rights Groups Call for Protection of Democracy and Privacy as Tech Responds to Pandemic," New America, June 11, 2020, https://www.newamerica.org/oti/press-releases/civil-rights-groups-call-protection-democracy-and-privacy-tech-responds-pandemic/

109 "E-GOVERNMENT ACT OF 2002," The United States Department of Justice, Feb. 23, 2021, https://www.justice.gov/opcl/e-government-act-2002

110 "Privacy Impact Assessment (PIA)," NASA, July 31, 2020, https://www.nasa.gov/sites/default/files/atoms/files/covid_19_contact_tracing_sdh.pdf

111 "ALGORITHMIC IMPACT ASSESSMENTS: A PRACTICAL FRAMEWORK FOR PUBLIC AGENCY ACCOUNTABILITY," AINOW, Apr. 2018, https://ainowinstitute.org/aiareport2018.pdf

112 "Privacy Considerations in Higher Education Online Learning: Privacy Policies and Practices," New America, Oct. 26, 2020, https://www.newamerica.org/oti/reports/privacy-considerations-higher-education-online-learning/privacy-policies-and-practices

113 "How AI can spot cheating without breaching student privacy," Rewire Mag, 2020, https://rewire.ie.edu/ai-spot-cheating-breaching-student-privacy/

114 "Civil Rights Groups Call for Protection of Democracy and Privacy as Tech Responds to Pandemic," New America, June 11, 2020, https://www.newamerica.org/oti/press-releases/civil-rights-groups-call-protection-democracy-and-privacy-tech-responds-pandemic/

115 "Exploring the Twenty-First Century Privacy Debate," New America, Sep. 17, 2019, https://www.newamerica.org/oti/reports/exploring-twenty-first-century-privacy-debate/

116 "Family Educational Rights and Privacy Act (FERPA)," U.S. Department of Education,Dec. 15,

2020, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

117 "Glossary," U.S. Department of Education, Dec. 30, 2020, https://studentprivacy.ed.gov/glossary

118 "Edtech is surging and parents have some notes," TechCrunch, June 9, 2020, https://techcrunch.com/2020/06/09/edtech-is-surging-and-parents-have-some-notes/

119 "Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students," Federal
Bureau of Investigation, Sep. 13, 2018, https://www.ic3.gov/Media/Y2018/PSA180913

120 "To amend the Family Educational Rights and Privacy Act of 1974 to ensure that student data handled by private companies is protected, and for other purposes.," Ed Markey: United States Senator for Massachusetts, July 14th, 2017, https://www.markey.senate.gov//imo/media/doc/2014-07-14_StudentPriv_BillText.pdf

121 "FERPA & Coronavirus Disease 2019 (COVID-19) Frequently Asked Questions (FAQs)," U.S. Department of Education, Mar. 2020, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf

122 "FERPA & VIRTUAL LEARNING DURING COVID-19," U.S. Department of Education, Mar. 30, 2020, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAandVirtualLearning.pdf

123 "Governor Cuomo Signs Legislation Suspending Use and Directing Study of Facial Recognition Technology in Schools," New York State Governor Andrew M. Cuomo, Dec. 22, 2020, https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-suspending-use-and-directing-study-facial-recognition

124 "How well do IBM, Microsoft, and Face++ AI services guess the gender of a face?," Gender Shades, Feb. 9, 2018, http://gendershades.org/

NEW AMERICA