

# Online and Observed\_

**Student Privacy Implications of  
School-Issued Devices and Student  
Activity Monitoring Software**



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



# Online and Observed

## Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software

### Authors

**DeVan L. Hankerson**

**Cody Venzke**

**Elizabeth Laird**

**Hugh Grant-Chapman**

**Dhanaraj Thakur**

### WITH CONTRIBUTIONS BY

L. Holden Williams, Bex Montz, Hannah Quay-de la Vallee, Samir Jain, and Timothy Hoagland.

### ACKNOWLEDGEMENTS

We thank all the local education agencies we interviewed who generously shared their time and insights to help inform our analysis. We also thank the various researchers and non-profit organizations who provided guidance and shared their best practices with our team.

### SUGGESTED CITATION

Hankerson, D.L., Venzke, C., Laird, E., Grant-Chapman, H., Thakur, D. (2021) Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software. Center for Democracy & Technology. <https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/>.



# Contents

<b>Executive Summary</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
<b>Main Findings / Discussion</b>	<b>8</b>
Finding #1: Students using school-issued devices are monitored to a greater extent than their peers using personal devices.	8
Finding #2: LEAs with wealthier student populations reported that their students are more likely to have access to personal devices, which are subject to less monitoring than school-issued devices.	10
Finding #3: LEAs feel compelled to monitor student activity to satisfy perceived legal requirements and protect student safety.	11
Finding #4: Most prevalent community concerns were focused on appropriate use of student activity monitoring data for disciplinary purposes.	12
Finding #5: LEAs communicate privacy expectations to students and families, but are unsure about how much detail about student activity monitoring to include in those messages.	14
Finding #6: LEAs are holding device and student activity monitoring software vendors accountable on privacy and security through data sharing and privacy agreements.	16
Finding #7: LEAs are looking for ways to improve the privacy and security protections for devices and data shared with student activity monitoring vendors.	18
<b>Conclusion</b>	<b>20</b>
<b>Methodology</b>	<b>21</b>
<b>References</b>	<b>22</b>

# Executive Summary

**M**any school districts across the nation expanded efforts to provide devices like laptops and tablets to students during the global pandemic in an effort to close the homework gap and address inequities in technology access. Part of this shift included the introduction of student activity monitoring software and other digital tools aimed in part at facilitating remote classroom management and driving student engagement. However, these tools can also be used in ways that are unduly intrusive. In this report, we examine whether students who receive school-issued devices are subject to more monitoring than their peers who have their own devices. We also examine local education agencies' motivations in implementing monitoring and how they communicate about it with parents and students.

Building on recent CDT guidance on how schools could address privacy gaps in the implementation of remote education technology (Quayde la Vallee & Venzke, 2020), this report presents findings based on virtual semi-structured interviews with nine individuals from five local education agencies (LEAs), including district level administrators and information technology (IT) directors.

This research uncovered seven main findings:

1. Students using school-issued devices are monitored to a greater extent than their peers using personal devices;
2. LEAs with wealthier student populations reported that their students are more likely to have access to personal devices, which are subject to less monitoring than school-issued devices;
3. LEAs feel compelled to monitor student activity to satisfy perceived legal requirements and protect student safety;
4. Most prevalent community concerns were focused on appropriate use of student activity monitoring data for disciplinary purposes;
5. LEAs communicate privacy expectations to students and families, but are unsure about how much detail about student activity monitoring to include in those messages;
6. LEAs are holding device and student activity monitoring software vendors accountable on privacy and security through data sharing and privacy agreements; and
7. LEAs are looking for ways to improve the privacy and security protections for devices and data shared with student activity monitoring vendors.



# Introduction

As advocates have increasingly called for reforms to address educational inequities exacerbated by the global pandemic, K-12 schools across the country have reexamined and taken action to address the inequitable results that may arise from the reliance on data and technology in education. In particular, they prioritized closing the homework gap — the 15 to 16 million American students who do not have broadband access at home — as remote learning was the only educational option available to many students. These efforts resulted in a dramatic increase in the percentage of students using school-issued devices. According to CDT research, 86% of teachers reported that, during the pandemic, schools provided tablets, laptops, or Chromebooks to students at twice the rate (43%) prior to the pandemic, an illustration of schools' attempts to close disparities in digital access. (Center for Democracy & Technology, 2020)

One technology application facing increased scrutiny as more students are using school-issued devices is software that monitors student activity. With the advent of new technologies and the expansion of remote learning, schools have increasingly deployed technically sophisticated means of monitoring and directing students' online activity (Center for Democracy & Technology & Brennan Center for Justice, 2019a), which may permit them to see what applications or websites students have open. It also allows schools to launch websites, switch tabs, block sites, or view browsing histories. This software is criticized due to questions about its efficacy, invasive privacy violations, and potential chilling effect on students' willingness to express themselves. (Center for Democracy & Technology & Brennan Center for Justice, 2019b)


**CDT sought to understand the scope and impact of the use of monitoring software on school-issued devices.**



Given this, CDT sought to understand the scope and impact of the use of monitoring software on school-issued devices. We conducted online semi-structured interviews with nine school officials in five diverse local education agencies (LEAs).


Our interviews suggest that students using school-issued devices are monitored to a greater extent than students using personal devices. That accords with national survey data produced by CDT, in which 71% of teachers report that their school or district uses student activity monitoring software on school-issued devices, as compared to 16%

**We conducted online semi-structured interviews with nine school officials in five diverse local education agencies (LEAs).**



of teachers who report use of this software on students' personal devices. (Center for Democracy & Technology, 2021b) Moreover, LEAs with higher-poverty student populations reported in interviews that a greater number of their students relied on school-issued devices and, therefore, were more likely to face increased levels of online activity monitoring by their schools. Our research also sought to understand why schools turn to monitoring software and discovered a variety of motivations, including perceived legal requirements.

Many types of technology collect information on students and could be categorized as “monitoring” technologies. This report does not address the full breadth of every technology that could be labeled “monitoring” software but focuses on “monitoring” in two senses: (a) technology that collects data on individual students, such as a learning management system logging when students use the system or a webapp scanning students' email messages; and (b) software on school-issued devices that allows for real-time features, such as viewing students' screens or switching which applications they have open.



# Main Findings / Discussion

**C**DT interviewed administrators at five LEAs, encompassing a diverse set of geographies and student bodies, to understand how student activity monitoring software is used at the K-12 level and how it impacts students who rely on school-issued devices compared to their peers who use their own personal devices for school purposes. Based on this research, CDT identified seven key findings:

**Finding #1: Students using school-issued devices are monitored to a greater extent than their peers using personal devices.**

The mechanisms and extent of monitoring student activity differ in important ways when comparing school-issued and personal devices (e.g. devices that the student and/or their family own). Although LEAs report security benefits to using school-issued devices, these divergent experiences suggest that students using school-issued devices are monitored to a greater extent than their peers using personal devices.

LEAs see some student safety and data security benefits in using school-issued devices. They describe school-issued devices as a more efficient and effective way to protect student security, highlighting potential harms to students from outside threats. According to LEAs, providing security for school-issued devices is easier because they provide a consistent hardware and software ecosystem. According to one administrator, “There’s a lot to be said about the district-issued device, the security around that device, and the sustainability of being able to manage that device effectively.”

However, for students using a school-issued device or hotspot, web-browsing activity and online behavior may be monitored through their use of the device’s internet browser, by software or applications installed on the device, or through the hotspot provided for internet connectivity. The degree of monitoring on school-issued devices can be constant and pervasive. One administrator described the level of monitoring as follows:

*[Students’ online] traffic 24/7 is going through our web filter... There’s no limitation on that. If they’re on our device, it doesn’t matter what time of day or what day of the week — their traffic is going through our web filter.*



In contrast, students using a personal device and their own internet connection may only be monitored when logging into an LEA-provided portal or application, or a browser using school credentials.

One participant summarized, “If that student is on their own device at home and they’re using their own wireless access, the only way we would control them at that point is if they logged into our portal.” The portal or LMS allows LEAs to have some visibility into student activities on a personal device but it is primarily limited to actions and information recorded within the specific application, which can include data about the type of device a student is using, submitted assignments, chat-related activity, or outreach to teachers.

Similarly, a student logged into a browser using their school credentials on a personal device is subject to monitoring that may be comparable to that of a student using a school-issued device. In explaining this kind of monitoring, one participant said:

*If I’m a student [in this LEA and] I log in to my [student] account on a browser on a personal computer, what I’m doing now ... while logged in on that browser would be [monitored] the same as if I run a district-owned [device].*

Despite potential monitoring through an LEA-provided application or browser, personal devices are generally subject to less monitoring than school-issued devices. This is in part due to the comparatively deeper level of technical access school-issued devices provide to school administrators, which allow them visibility into a broader array of student behavior, as discussed above.

**“If a student has their own device, [my view is that]...I’m not your parent, so I’m not going to monitor anything that you do on your own device.”**

However, some participants also cite perceived norms around the extent of their appropriate administrative roles with respect to monitoring. One participant pointed out that:

*If a student has their own device, [my view is that]...I’m not your parent, so I’m not going to monitor anything that you do on your own device.*

In sum, monitoring on school-issued devices is more granular and continuous. While some forms of activity tracking occur on personal devices, the predominant view among LEA administrators was that activity on personal devices fell outside the scope of their responsibility to review.

## Main Findings / Discussion

### **Finding #2: LEAs with wealthier student populations reported that their students are more likely to have access to personal devices, which are subject to less monitoring than school-issued devices.**

Local education agencies with wealthier student bodies were more likely to describe student use of their personal devices in remote learning settings. “We have seen this, especially during the pandemic, where we may issue a device for the student, [they] take it home, and they pretty much put it on the shelf because they’d rather use their [own] device,” said one district official in one of the wealthiest LEAs examined.

In LEAs with higher-poverty student populations, the experience with personal devices differed in two key aspects: first, administrators reported lower overall use of personal devices. For example, in providing a breakdown of what proportion of students were currently using devices from the district, one participant from an LEA with a higher-poverty student body indicated that school-issued devices are used by nearly every student in the district. They described that:

*Every student has the opportunity to use a device in the district. Now, from a percentage standpoint, I would probably be safe in guessing around 98 or 99 percent [of the student population use school-issued devices], with the understanding that some parents may have chosen not to use the school-issued device and they wanted to use their own device, for whatever reason.*

Second, at least one LEA reported that they encouraged students to use school-issued devices by making it easier for students to access synchronous instruction on these devices.

They recounted:

*We know that there are students who use home devices for [the LMS tool], for example ... but because [the videoconferencing and messaging tool] has been the primary way that we have done synchronous communication, we know that almost all of our students are using their district-issued computer for [those purposes] at least ... that client is already installed and it’s single sign on. It’s really easy for them to use.*

In other words, students in this higher-poverty LEA will find that it is much easier for them to rely on the school-issued device alone. As discussed in Finding #1, most of the LEAs surveyed reported continuous monitoring on school-issued devices and, by

comparison, characterized student activity monitoring on personal devices as occurring only with use of district credentials on digital platforms or software tools. This indicates that students who are reliant on school-issued devices may be subject to more pervasive monitoring. The first two findings taken together suggest that students in lower-income districts may be subjected to a higher degree of monitoring than students in wealthier districts, who are more likely to make use of personal devices.

**Finding #3: LEAs feel compelled to monitor student activity to satisfy perceived legal requirements and protect student safety.**

All of the districts interviewed for this research had adopted and implemented some form of student activity monitoring software for their student populations. One of the primary factors driving LEAs to implement student activity monitoring software is to satisfy perceived legal and funding requirements. A common belief among district participants was that student activity monitoring software was required for compliance with the Children’s Internet Protection Act (CIPA) and the Family Educational Rights and Privacy Act (FERPA), and for accessing funding through the E-Rate program.<sup>1</sup> LEAs were explicit, saying, “our approach was [that] we needed a lot of granular control so that we would comply with CIPA.” Another said:

*I think our posture was not, “Hey, we need to go get software that monitors the activity of students.” Our posture came out of we’re required by CIPA to do certain things...that is a requirement of the E-Rate. We do participate in E-Rate, so we are completely following those rules and regulations. [And] FERPA [sic].*

Beyond compliance with CIPA, many LEAs described the primary benefit of using student activity monitoring software as helping ensure student safety. LEAs mentioned that student activity monitoring software allowed them to track student engagement, which was necessary in distance learning settings, as well as measure progress and attendance. Administrators also cited protection from malicious external threats as another advantage, citing software features that identify unusual activity, suspicious IP addresses, and compromised accounts. LEA officials went on to explain that educational data and student information are high-value targets for malicious actors, and several participants described the consequences for student victims of identity theft.

---

1 CDT has concluded that the “monitoring” requirement under CIPA is limited in scope (Center for Democracy & Technology, 2021). Although FERPA’s privacy protections apply to the use of student activity monitoring software, the statute does not require its use.

## Main Findings / Discussion

In addition to guarding against the harms of data breaches, LEAs also reported that they seek to use student activity monitoring to protect students' physical and mental health. In discussing why they decided to seek out student activity monitoring tools, one administrator talked about interrupting students' attempts to self-harm:

*We knew that there were students out there having ideations around suicide, self-harm and those sorts of things. As we started looking for a tool, we found this [student activity monitoring software]. We could also do a good job with students who might be thinking about bullying....It doesn't really matter what it costs, because if I can save one student from committing suicide, I feel like that platform is well worth every dime that we paid for [it].*

The dominant view among LEA officials of student activity monitoring software was that it protects students from these and other potential sources of harm. Additionally, national survey research done by CDT found that 78% of teachers and 75% of parents strongly or somewhat agree that student online activity monitoring keeps students safe by identifying problematic online behavior, such as visiting websites about mass shootings, searching for instructions on how to harm themselves, or identifying images that suggest substance abuse. (Center for Democracy & Technology, 2021b)

Participants also made sure to clarify what they perceived as an expansion of their capacity to keep students safe because of student activity monitoring software. One participant said:

*I want to be clear about the fact that we don't monitor students for the sake of monitoring, and what [student activity monitoring software] has helped us to do this school year...has been pretty profound during a time where students were struggling emotionally.*

In sum, LEAs cited protecting students as a primary benefit that led them to procure student activity monitoring tools.

### **Finding #4: Most prevalent community concerns were focused on appropriate use of student activity monitoring data for disciplinary purposes.**

LEAs reported that their community members were most concerned with the use of student activity monitoring software pertaining to student discipline. When asked whether members of the larger school community had expressed direct concern about the use of student activity monitoring software, LEA administrators responded that

community members were supportive of student surveillance in many cases, but they also noted some worries about how LEAs used discipline data. Parents asked whether discipline data was shared with state agencies and about how these agencies used this information. One participant said:

*The conversations we've had with parents with regard to privacy have been around how student data is used within our system, but also as that data is moved to the state, for example. We have parents concerned [that]...a discipline incident in third grade, is going to follow that student into junior high, and high school, and that's going to impact their ability to be successful....*

Other LEAs discussing student activity monitoring tools in disciplinary contexts explained what they saw as an opportunity to provide thoughtful review of student behavior using data proactively, as opposed to relying on “snap” disciplinary decision-making. According to one official, monitoring student activity allows administrators to establish a pattern of behavior using data, to preempt worse student behavior, and to witness behavior in real time:

*[Data from these tools] could be used for disciplinary actions. We're dealing with a couple of incidents right now where schools have asked us to do some investigation into potential inappropriate use of technology... [I]t also gives us a chance to go back and look at anything that might've been questionable in terms of the activities that took place and are being investigated.*

**“We are actually having some pretty big meetings right now to discuss how we evaluate the concerns that come from [student activity monitoring software] and escalate them more thoughtfully...”**

On this question of how to respond to student behavior flagged by student activity monitoring software, some LEAs described the inherent difficulty in determining proportional responses. As an example, one participant noted that some online behavior flagged by the software sometimes escalates, raising challenging questions about how schools interact with law enforcement:

*There is a very fine line in determining in a student communication what they mean by, “I am going to kill someone,” for example. We are actually having some pretty big meetings right now to discuss how we evaluate the concerns that come from [student activity monitoring software] and escalate them more thoughtfully... [We are] trying to make sure that we are doing that thoughtfully and in a way that respects families' concerns about the relationship of school and police departments.*

## Main Findings / Discussion

**"... As part of our communications with students and our student family handbook, there is a statement...that there is no expectation of privacy."**

**Finding #5: LEAs communicate privacy expectations to students and families, but are unsure about how much detail about student activity monitoring to include in those messages.**

LEAs explicitly communicate to students and families that there is no expectation of privacy when using school-issued devices and when operating on school-provided networks. However, LEAs also state they are committed to protecting student privacy, as stated in school materials, which may indicate that these commitments are intended to refer only to external privacy threats. One LEA administrator outlined their stance on the expectation of privacy:

*... As part of our communications with students and our student family handbook, there is a statement...that there is no expectation of privacy.*

With the exception of discipline data noted above, LEAs generally characterized community concerns surrounding the use of student activity monitoring software as fairly minor. However, they also outlined the tension LEAs face around providing transparency on student activity monitoring. In discussing what it would take to help families develop a thorough understanding of what kind of information student activity monitoring tools collect, one administrator said that, "Families are not as actively concerned about that...and it is an interesting challenge for me personally of wanting to give families more information, but also not wanting to stir the pot."

In addition to sharing information about student activity monitoring with parents, LEAs also reported concerns about being transparent with students. Participants described a primary concern with the use of student activity monitoring software to be students' abilities to circumvent and undermine the LEA's safety efforts. Participants in this study described this concern:

*The challenge is that [student activity monitoring is] only one solution. So, if a student knows that they're being specifically monitored because there's a concern and they just say, "Well, I'll just use my personal cell phone that's [not] on the district network," then they've...circumvented any kind of precautions that we have in place.*

In raising this issue, another LEA official explained that they de-emphasized communications to the student body about these tools, deciding not to "campaign" about the use of monitoring software to avoid increasing the likelihood of circumvention by students. District officials raised the possibility that student

**Another LEA official explained that they de-emphasized communications, deciding not to “campaign” about the use of monitoring software to avoid increasing the likelihood of circumvention by students.**

awareness of activity monitoring might lead students to reconsider discussing suicidal ideation using district-provided computing tools, for fear of being discovered. In their view, high levels of student awareness of monitoring would somewhat diminish the value of student activity monitoring, specifically the capacity to manage student safety and take pre-emptive action. This anecdotal awareness of the potential for a chilling effect is supported by national survey research which shows that of students who indicate that their school uses student activity monitoring software, 80% report being more careful about what they search for online when they know they are being monitored. (Center for Democracy & Technology, 2021b)

One administrator expressed concerns that students may attempt to subvert safety measures, which could thwart the district’s efforts to provide necessary support and interventions to students struggling with suicidal ideation:

*I want a child to use the devices that we’ve given them. So, if I tell a student, ‘I can catch you...we’re monitoring you,’ that child may never use that [device] to talk about her or his ideations about suicide. I think that’s just a really good example of why we don’t make a big deal about trying to let the entire community know how and what we’re using for monitoring.*

Anecdotes like this illustrate some LEAs’ rationale for opting to limit the degree of public messaging around their use of student activity monitoring software.

Disclosures about data protection, student data sharing policies, and data security related to the use of student activity monitoring software varied between LEAs. Some LEAs provide granular-level details on data sharing practices, including data elements being exchanged with software vendors, and they publish vendor contracts online. Others reported that their communications about district data privacy and security regulations were fairly new, drafted in response to the shift to remote learning due to COVID-19. And yet others felt they should try to meet a higher standard of transparency because of the scope of activity monitoring happening with the use of specific online monitoring tools.

In answer to questions about how LEAs might improve implementation of student activity monitoring tools, one participant talked about the opportunity available to LEAs to expand communications with the school community:

*There is still a huge opportunity for us to be even better about our communication to parents and to drive better understanding about why schools might be using [student activity monitoring tools] and also really what is being monitored. Because again, there has not been significant pushback on this, but I also don’t think that people maybe have fully understood.*

## Main Findings / Discussion

### **Finding #6: LEAs are holding device and student activity monitoring software vendors accountable on privacy and security through data sharing and privacy agreements.**

LEAs hold third-party vendors accountable to protecting privacy and security by using data sharing and privacy agreements. Many of these standard agreements include addenda with specific provisions related to the software type or software vendor in question. These agreements include start and end dates, details on data handling, and specifics about the disposition of the data once the agreement has ended, among other things. One of the ways LEAs say they protect student privacy is by giving preference to data sharing and privacy agreements developed by district counsel rather than vendor-provided agreements when possible.

In negotiating these agreements, LEAs reported several items they wished to see represented in the document text including further detail on:

- *Data ownership* – Who owns the data?
- *Data retention* – How long is that data in the possession of the software vendor once the contract has ended?
- *Data control and access* – Who has control of and access to the data and what roles do they occupy within the vendor’s company? What level of data access is provided, and what, if any, encryption or scrambling is applied to the data?
- *Specific knowledge of technical systems* – What systems are in use?
- *Further detail on geographic boundaries* – Where are data centers located? Are they in the U.S. or abroad?

Some district administrators expressed frustration with the power imbalances between LEAs and large tech companies in negotiations over data sharing and privacy agreements. They felt they were operating at disadvantage and that there was a perception among large tech companies that their privacy agreements should be privileged over an agreement provided by the LEA.

Specifically regarding student activity monitoring software vendors, LEAs mentioned the importance of ensuring vendor capacity to protect student data as well as implement privacy- and security-forward data handling practices. Unlike previous uses of school technology, which relied on the school’s direct oversight to ensure adequate protection, district administrators today have to use different tools to ensure vendors manage data appropriately. The administrator noted:



*One of the biggest challenges...[is that our students' data is] not on our servers like it used to be in the old on-[premises] days. We have language in place to protect the data [such] that they don't share it while they have it on their servers.*

Our research indicates that in the software procurement process, LEAs take active steps to prioritize data privacy, particularly as it relates to student activity monitoring software. LEAs report stark differences in the degree to which they are able to prioritize privacy protection in the procurement of hardware versus software.

Despite the disproportionate monitoring of students using school-issued devices, LEAs report that they are unable to prioritize privacy and security when procuring devices. Even where there is a focus on privacy, device vendors' privacy and security standards remain a key challenge for LEAs as they navigate device procurement, primarily due to what they describe as a lack of distinguishable options for privacy-forward devices. LEA officials report that computing devices do not specifically incorporate standalone privacy features that would exist apart from the privacy-protective measures embedded into the accompanying operating system or software. As described in Finding #7 below, LEAs tend to emphasize privacy in procuring *software* services to a greater extent than in their approach to device procurement.

In contrast to limited options available for privacy protection when making hardware decisions, LEAs find they have a wider range of strategies available to ensure strong privacy practices in software selection and adoption.

District officials cite a number of changes in software procurement processes implemented in the past few years, most of which aim to improve software vetting and data privacy protections. These have included implementation of a committee-review, which invites input from multiple departments in addition to IT staff.

Other improvements, like data minimization, are executed in the boilerplate language of district data sharing agreements. Also, LEAs say that they have become much more practiced over time in their negotiations with software vendors. For example, common practice is now to settle critical questions about data handling and security ahead of the contract phase. One major caveat of these provisions, however, is that LEAs have limited visibility into vendor-side systems operations, which makes it difficult to conduct independent audits for compliance with the terms of a given agreement.

## Main Findings / Discussion

### **Finding #7: LEAs are looking for ways to improve the privacy and security protections for devices and data shared with student activity monitoring vendors.**

Given the concerns raised by LEAs about the privacy and security risks associated with both school-issued devices and the use of student activity monitoring software, the participants pointed to approaches they are considering, which they believe can reduce risks posed by unauthorized access to devices.

In discussing some of the ways the device procurement process could incorporate a stronger focus on privacy, LEAs talked about device-specific options that could enhance security for device access. Some LEAs mentioned the potential to use biometric technology as a means to prevent unauthorized access to school-issued devices — fingerprint readers were cited as one such example. However, participants also expressed concerns that a lack of familiarity with this technology among students, parents, teachers, and the wider school community could present a barrier to its effective use.

While discussing how implementation might take place, one official relayed that parents would have no frame of reference for this type of technology and would likely be skeptical if it were introduced:

*We have a tough enough problem right now, trying to prove to outsiders that we are protecting their data. So when we start talking about biometrics and giving up that kind of information, it may be a challenge for us.*

Another approach one district suggested was to deploy multi-factor authentication, particularly for use with middle and high school students, again as a way to better secure school-issued devices.

LEAs are also considering ways to improve privacy and security protections for data shared with student activity monitoring vendors. Participants reported a consensus among peers about the necessity to protect student data shared with vendors. For example, some LEAs pointed to the need for measures to be taken by vendors to prevent unauthorized access to student data particularly following the termination of contracts between the two parties. Legal protections that would prohibit vendors from creating off-server copies of student data, as well as affirmative declarations from vendors that student data has been deleted once a district has ended their engagement, were cited as useful provisions.

Administrators went on to say that smaller, newer software vendors offer fewer options for cloud data encryption, posing a potential challenge. By comparison, larger companies have the financial capability to provide robust encryption solutions. Finally, they also suggested that including requirements for vendors on encryption standards for data at rest and in transit could be a helpful measure for privacy protection.



## Conclusion

**W**ith the expansion of school-issued devices and student activity monitoring software, this study examined their impact and whether student recipients of school-issued devices were subject to more monitoring than their peers using devices that they or their families own. Based on reports from LEAs, it would appear that students using school-issued devices are subject to more monitoring than their peers using personal devices.

Additionally, our study identified important strengths, challenges, and future issues for policymakers and practitioners to consider in their efforts to close the homework gap while protecting student privacy.



# Methodology

The data collection and analysis for this report was conducted by CDT and took place between April and June 2021. It is based on five LEAs across the U.S. Our aim was to include a broad range of experiences and locations. In terms of enrollment, the LEAs we interviewed ranged in size from 7,000 to almost 80,000 students. Other factors that we used to ensure diversity in our LEA sample pool include student population poverty rates (ranging from 12 percent to 30 percent) and racial demographics (the percentage of the student population that is white ranged from 13 percent to 72 percent).<sup>1</sup> Finally, four out of five of the LEAs currently operate on a 1:1 model for providing school-issued devices to their student populations.

We conducted online semi-structured interviews with nine individuals from these LEAs, which included district-level administrators and IT directors. The interviews, which lasted between 60 and 90 minutes each, covered a range of topics including comparisons between school-issued and personal devices, device distribution policies, the use of student activity monitoring software, and training and digital literacy. All interviews were done on a voluntary basis.

All the interviews were recorded and transcripts were used for analysis. A coding scheme was developed based on the main research question of differences in privacy risks between school-issued and personal devices. Several rounds of coding were completed to yield the analysis summarized in this report. Finally, for each LEA we also collected and reviewed publicly available privacy policies, data sharing agreements, and other relevant documentation to support our analysis.

While this study provides some perspective on LEA administrators' view of activity monitoring tools and vendors, as well as student data and privacy, these findings are limited to the views of the five participating LEAs. Further, this research does not discuss potential solutions to some of the challenges posed within this report. For more information on actions that policymakers and practitioners can take, please see CDT's two-pager *Student Activity Monitoring Software: Research Insights and Recommendations* and our issue brief *Closing the Homework Gap While Protecting Student Privacy*.

---

1 Poverty rates refer to “percentage of families and people whose income in the past 12 months is below the poverty level” within the school district. (National Center for Education Statistics, 2019) For one of the LEAs (a charter school) the poverty rate refers to the percentage of students who qualify for free or reduced lunch. It was 70%. For LEAs (with the exception of the charter school included in this study) the percentage of the population that identifies as white refers to rates within the LEA. (National Center for Education Statistics, 2019)



# References

- Center for Democracy & Technology. (2020). *Protecting Students' Privacy and Advancing Digital Equity* (pp. 1–6). Center for Democracy & Technology. <https://cdt.org/insights/research-report-protecting-students-privacy-and-advancing-digital-equity/>
- Center for Democracy & Technology. (2021a). *With Increased EdTech Comes Increased Responsibility* (pp. 1–6). Center for Democracy & Technology. <https://cdt.org/insights/research-report-with-increased-edtech-comes-increased-responsibility/>
- Center for Democracy & Technology. (2021b). *Student Activity Monitoring Software: Research Insights and Recommendations* (pp. 1–3). Center for Democracy & Technology. <https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations/>
- Center for Democracy & Technology & Brennan Center for Justice. (2019a). *Technological School Safety Initiatives: Considerations to Protect All Students* (pp. 1–3). Center for Democracy & Technology. <https://cdt.org/insights/technological-school-safety-initiatives-considerations-to-protect-all-students/>
- Center for Democracy & Technology & Brennan Center for Justice. (2019b). *Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns* (pp. 1–5). Center for Democracy & Technology. <https://cdt.org/insights/social-media-monitoring-in-k-12-schools-civil-and-human-rights-concerns/>
- National Center for Education Statistics. (2019). *The American Community Survey – Education Tabulation (ACS-ED)*. U.S. Department of Education. Institute of Education Sciences, National Center for Education Statistics. <https://nces.ed.gov/programs/edge/Demographic/ACS>
- Quay-de la Vallee, H., & Venzke, C. (2020). *Privacy and Equity in the New School Year*. Center for Democracy & Technology. <https://cdt.org/insights/report-privacy-and-equity-in-the-new-school-year/>