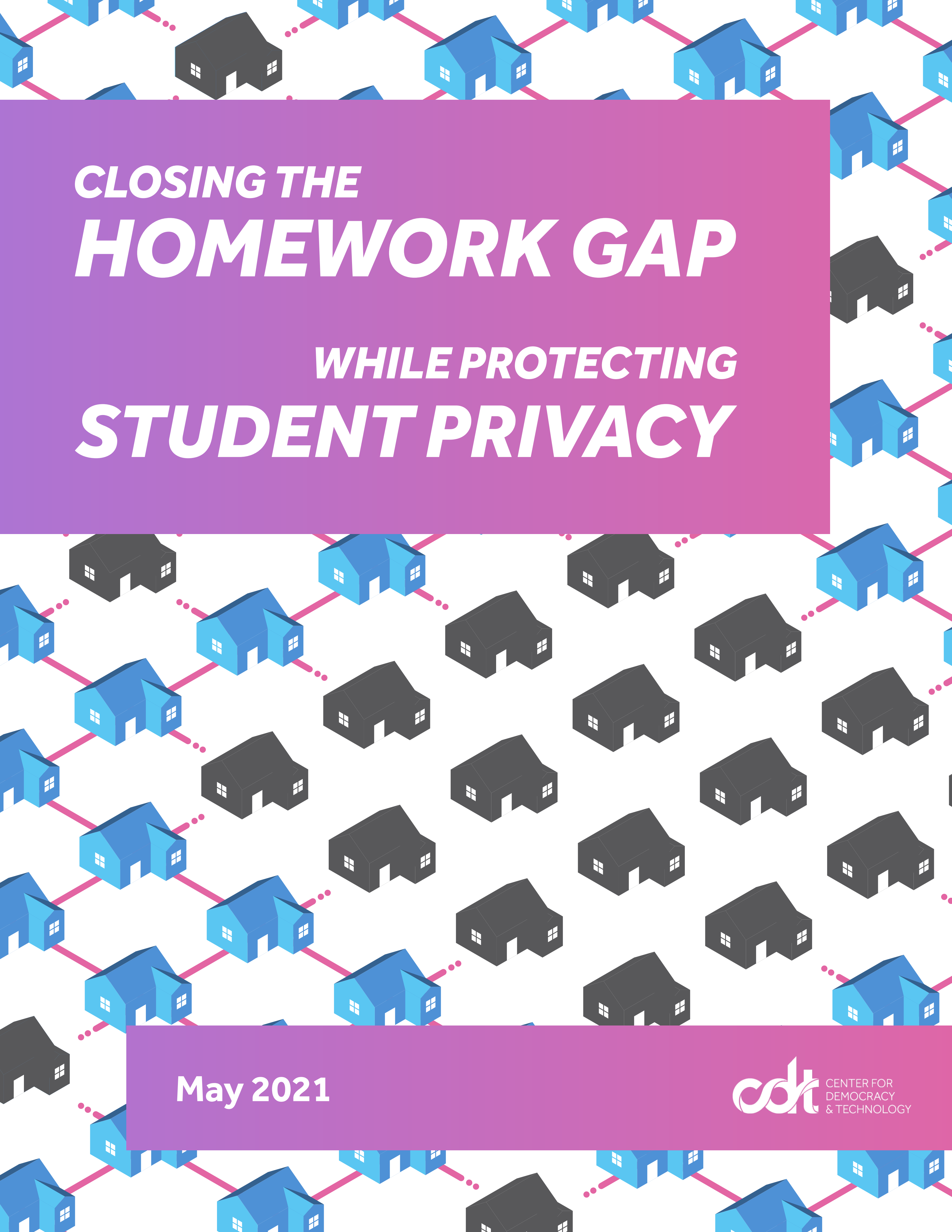

CLOSING THE HOMEWORK GAP WHILE PROTECTING STUDENT PRIVACY

May 2021

CENTER FOR
DEMOCRACY
& TECHNOLOGY

About the Center For Democracy & Technology

The Center for Democracy & Technology is a 501(c)(3) working to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. Based in Washington, D.C., and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to today's most pressing technology policy challenges. Our team of experts includes lawyers, technologists, academics, and analysts, bringing diverse perspectives to all of our efforts. Learn more: cdt.org/

About Student Privacy

CDT's vision for the Student Privacy Project is to create an educated citizenry that is essential to a thriving democracy by protecting student data while supporting its responsible use to improve educational outcomes. To achieve this vision, CDT advocates for and provides solutions-oriented resources for education practitioners and the technology providers who work with them, that center the student and balance the promises and pitfalls of education data and technology with protecting the privacy rights of students and their families.

About Equity In Civic Tech

As governments expand their use of technology and data, it is critical that they do so in ways that affirm individual privacy, respect civil rights, foster inclusive participatory systems, promote transparent and accountable oversight, and advance just social structures within the broader community. The Equity in Civic Technology Project at CDT furthers these goals by providing balanced advocacy that promotes the responsible use of data and technology while protecting the privacy and civil rights of individuals. We engage with these issues from both technical and policy-minded perspectives, creating solutions-oriented policy resources and actionable technical guidance.

AUTHORED BY

Cody Venzke, Policy Counsel, Equity in Civic Technology Project
Hannah Quay-de la Vallee, Senior Technologist

Closing the Homework Gap While Protecting Student Privacy

Executive Summary

As institutions at all levels of government and across our communities work to connect students to remote learning, those efforts should not come at the expense of student privacy. Closing the homework gap — the 15 to 16 million American students who do not have broadband access at home — will likely require schools to utilize data and technology in new and unexpected ways, presenting new challenges to both equity and student privacy. When closing the homework gap, those challenges are likely to arise in five areas:

- **Using Data to Assess Needs and Launch Connectivity and Device Programs.** Schools may collect data from or about students to better understand whether they lack broadband, and if so, why. That data collection, however, may pose a risk to both community trust and student privacy if data is used in unexpected ways.
- **Sharing Student Data with Third Parties Such as Broadband and Device Providers.** In getting students connected, schools may have to share data with broadband and device providers or other third parties for several reasons, including to provide connectivity, devices, or services, or to more efficiently administer or implement a broadband or device program. That sharing may pose risks to student privacy and equity if schools are unable to ensure their partners use the data responsibly.
- **Monitoring Student Activity Online.** With the advent of new technologies and the expansion of remote learning, schools have increasingly deployed technically sophisticated means of monitoring students' online activity, which may permit teachers to see what students have open on their computer screens, open websites on a student's laptop, switch tabs, block sites, or view browsing histories, which can jeopardize students' privacy or cause equity concerns if this surveillance falls disproportionately on minority communities.
- **Ongoing Security and Device Management Requirements.** Distributing devices to students comes with an added responsibility to minimize the potential for harm that can come with those devices, as they can be a pathway for attacks on student privacy.
- **Lack of Digital Literacy and Security Knowledge.** Students and families, especially those who are new to the digital space, may lack the digital skills and experience necessary to navigate privacy and security challenges.

The resulting challenges can include a lack of meaningful consent, secondary data uses, overcollection and indefinite retention of data, misuses of data, a loss of public trust, increased inequities, and legal risks. These serious risks, however, can be combated with privacy- and equity-forward practices. These practices will help center the student and community in the use of data and technology to close the homework gap, namely by:

- **Developing Robust Data Governance.** Schools should establish robust processes and structures for overseeing the overall management, availability, usability, integrity, quality, and security of data and technology.
- **Engaging the Community.** Schools should engage stakeholders such as students and families, teachers, and administrators — and even broadband providers and state education agencies — about the use of data throughout the process of closing the homework gap.
- **Complying with Legal Rules.** Schools opting to collect and share data face some legal risk, as federal and state privacy laws can be confusing and may not necessarily permit data sharing, so schools should ensure they work with legal counsel through the process of closing the homework gap.
- **Promoting Equity.** The use of data and technology has the potential to promote equity and limit biases, but only if the collection, analysis, and use of data is designed intentionally to meet these goals. Schools should focus on ensuring that data and technology used to close the homework gap do not reinforce the biases and inequities present in society, particularly in algorithmic applications.
- **Building Stakeholder Capacity and Digital Literacy.** Because data and technology are rapidly evolving, it is a challenge for organizations, especially those that are under-resourced, to have the capacity to enact and follow ethical data practices and policies. Organizations can build capacity by participating in trainings, creating guidance resources, and having dedicated staff to support community members.

Together, these practices can make it possible to close the homework gap while protecting student privacy.

Introduction

Not all students in the United States have reliable access to dedicated devices and the broadband connections that make remote learning possible, a fact that was brought into stark relief during the pandemic. Without broadband at home, some students were forced to connect to their lessons from McDonald's parking lots in the Mississippi Delta[1] or from churches in rural Nebraska.[2] In Arizona, some students drove across town to access Wi-Fi "beamed" from specially equipped school buses,[3] while in Appalachia, one student connected from mountaintops near her home, above the tree line where there is better cellular signal.[4]

According to the Federal Communications Commission, nearly a third of U.S. households lack access to broadband, a disparity known as the digital divide[5] — one that disproportionately affects Black, Latinx, low-income, and rural households.[6] Those households include 15 to 16 million school-aged children who lack reliable internet at home.[7] In the era predating the pandemic, that disparity prevented approximately 15 percent of students overall — and 35 percent from low-income families — from completing their homework.[8] Those students who cannot connect from home are on the wrong side of the digital divide and fall into the "homework gap."[9]

When schools moved online as a result of the pandemic, the homework gap became "especially cruel,"[10] and schools, families, and educators raced to get students online. In this issue brief, we highlight risks that well-intentioned efforts to close the homework gap may pose to both equity and student privacy. Closing the homework gap is essential for students' well-being, but so is protecting their privacy and access to equitable opportunities.

We focus on five areas that can pose risks to both equity and student privacy:

- Using data to assess needs and launch connectivity and device programs;
- Sharing student data with third parties such as broadband and device providers;
- Monitoring student activity online;
- Ongoing security and device management requirements; and
- Lack of digital literacy and security knowledge.

As described in this brief, schools can utilize practices and policies to mitigate the risks in each of these areas and advance equity and privacy.

Using Data to Assess Needs and Launch Connectivity and Device Programs

As schools shifted to remote learning, part of overcoming the challenges of the homework gap was using data to determine how to best help students access virtual learning while modeling best practices in how that data is used.[11] Collecting data can help facilitate understanding of not only which families lack broadband connections at home, but why. Those reasons can include a lack of infrastructure, affordability, and other barriers such as digital literacy or mistrust of broadband providers.[12] In Connecticut, the state's Commission for Educational Technology discovered that not all eligible families were taking advantage of free broadband supported by the state's Everybody Learns Initiative.[13] By collecting data through focus groups with district leaders who conveyed parent concerns, the Commission discovered that a variety of factors deterred parents from using the free broadband provided by the Initiative, including some that implicated student privacy such as worries about giving their information to third parties.

Privacy and Equity Risks

Assessing students' broadband needs is a data-heavy exercise and may require new collections or new uses of student data. The collection, retention, and use of sensitive data poses risks for schools, students, and families, such as:

- **Lack of Meaningful Consent:** There are important challenges to obtaining informed, meaningful consent. Meaningful consent means the user really reads and understands the ways their data may be used, and the user feels they have a meaningful, non-coerced choice in the data collection. However, that choice may not exist for a variety of reasons, including if a parent is forced to decide between disclosing information about their family so their student can receive educational services through a school-issued device or internet connection, or not disclosing that information and foregoing those services.
- **Overcollection of Information and Indefinite Data Retention:** In addressing a problem as complex as the homework gap, schools and stakeholders may be tempted to collect as much data as possible or to hold on to that data indefinitely. However, the more data that is collected and stored on students and their needs, the more risk there is for that data to be accidentally exposed or misused. Harm to students may result due to a data breach or even simply using the data outside its intended context.
- **Loss of Public Trust:** Overcollecting or failing to protect data may erode trust in the stewards of the data.[14] Loss of public trust can limit a school or organization's efficacy as well as its ability to understand and address community needs and concerns.

- **Legal Risk:** Federal and state law govern both the collection and sharing of student data, and schools collecting and using student data must ensure their collection and use comply with those legal requirements.
- **Lack of Capacity**: Institutions may not be transparent about how data is collected, stored, and used. Consequently, students and families may not be aware of data collections or uses, how to recognize misuses, or how to address or report data misuse.

Privacy-Forward and Equity-Forward Practices

To respond to those challenges, schools should employ the following three practices:

- Develop robust data governance;
- Engage the community; and
- Comply with legal rules, including the Protection of Pupil Rights Amendment (PPRA).

Develop Robust Data Governance

Data governance is "the overall management of data, including its availability, usability, integrity, quality, and security,"[15] and includes people, processes, and structures that are responsible for data and technology. When managing data that is collected to close the homework gap, data governance initiatives should address, at a minimum, the following issues:

- **Data Governance Structures:** Schools should establish a formal data governance structure for making decisions about student data that provides a mechanism to hear from the diversity of voices reflecting the populations being served and resolve any confusion or conflicts about decision-making. In the case of closing the homework gap, it is important to involve internal stakeholders who will manage and use this information (for example, edtech directors, chief information officers, local education agency data managers, service providers, state agencies, and community partners), as well as external stakeholders who play a role in providing and/or potentially being impacted by any data collections (for example, school, teachers, and families).
- **Data Minimization and Purpose, Use, and Access Restrictions:** In closing the homework gap, data governance plans should apply the principle of data minimization in which they collect, use, and disclose only the data that is necessary to getting students connected.[16] Schools should establish policy and technical controls to limit access to only individuals who have a clear need for it. Additionally, schools should place limitations on the sharing of data, discussed in the *Secure Collection, Storage, and Destruction Plans* section of this report.

- **Transparency**: The data collected, its intended uses, and any constraints on sharing should be publicly disclosed in a way that is accessible to diverse populations in the school community. For example, one state edtech commission collected data to better understand why families were not using subsidized broadband connections. The commission made the results transparent to the community and limited the use of the data to inform policy decisions.[17]
- **Secure Collection, Storage, and Destruction Plans:** Organizations should determine when and how data will be collected, stored, and destroyed securely.[18] Schools should ensure that any method used for collecting and storing data is secure, including the use of encryption technologies.[19] Data governance also should include plans for destroying data on an explicit timeline or when specified conditions are met, such as when a device is retired, and should consider legal requirements for retaining or destroying data. For a more in-depth discussion of this issue, see CDT's prior work on data destruction in education.[20]
- **Data Incident Response Planning:** As schools collect and share data, they and their partners should develop, implement, and practice data incident response plans.[21] The data incident protocol should define clear roles for relevant personnel at the school and any other partner who may have access to the data. Schools also should have plans to communicate (via written notice and possibly a meeting) with families, so they know if they were affected by an incident and where to go for further assistance. Having these plans in place can make for a more efficient and effective response to any incidents, rather than having to spend time after an incident trying to determine what to do.

Engage the Community

A loss of public trust stems, in part, from surprise and a lack of involvement in critical decisions about collecting, using, and sharing data.[22] As schools develop plans to collect student data to close the homework gap, they should engage stakeholders such as students and families, teachers, and administrators.[23] Doing so has multiple benefits, including ensuring that school initiatives meet community needs and build trust in the use of data and the organization more broadly. It can result in the early detection of concerns, a better understanding of the community's actual needs, and more inclusive and robust solutions.

Schools should engage both those who will use new data or repurpose existing information, such as broadband providers, public-private partners, and state agencies, as well as those about whom information is being collected, like parents and students. This engagement should inform decisions about what data is being collected, how it is being shared and used, and how it will be protected, retained, and eventually destroyed. Schools should proactively communicate with families, giving them necessary information to provide feedback and ensure transparency. Whenever possible, schools also should inform broadband providers of their privacy standards and information the school may be unwilling to share.

Engagement efforts should prioritize inclusivity and accessibility to ensure that parents and families across all backgrounds may participate.[24] This means meeting families where they are and providing effective engagement with parents and guardians who may work multiple jobs or evening and night shifts, speak a language other than English, have a disability, or lack access to transportation or broadband internet. For example, the Privacy Technical Assistance Center of the U.S. Department of Education recommends that schools document key aspects of programs for collecting and sharing student data and publish that documentation online[25]; those efforts should be accompanied by offline outreach such as telephone calls to engage families that lack broadband access, as well as publishing the documents in languages used by families throughout the district.

Comply with Legal Rules

Both state and federal law apply to schools' collection of student data to identify students' connectivity needs. These laws may require a school, at minimum, to provide parents with notice of new data being collected from students, to opt out of the collection, and to inspect the survey or tool used to collect the data. How these laws apply depends on who provides the data, so schools should be clear about who is supplying the information or consider alternative methods of assessing students' needs that do not involve collecting protected data. Importantly, although the pandemic has presented new challenges, the legal requirements around student privacy have not changed, and existing resources may guide schools through their legal compliance efforts.[26]

At the federal level, one law governing the collection of data is the Protection of Pupil Rights Amendment (PPRA).[27] The PPRA applies to "surveys" of students covering several subjects, including the family's income,[28] which schools may wish to collect to determine whether students qualify for subsidized or free broadband. If schools attempt to collect sensitive information like family income directly from students, they must provide notice of the survey to parents and give them an opportunity to opt out of its administration, assuming the survey is not mandatory.[29] Further, a student survey funded by the U.S. Department of Education covering a family's income may not be made mandatory for the student unless a parent first opts in.[30] Regardless of whether a survey is subject to the opt in or opt out requirement, a parent is always entitled to inspect a survey concerning protected topics listed in the PPRA.[31]

At the state level, more than 130 state student privacy laws have been passed since 2013.[32] Those laws' requirements can vary widely, and schools should consult with counsel before implementing a new data collection or use. For example, some schools have tracked students' activity in online lessons to identify students who were not connected[33]; Louisiana state law, however, prohibits an official or employee of any "local public school system" from collecting any of thirteen types of student information, including a student's "Home Internet Protocol Address" and "External digital identity" unless "voluntarily disclosed" by the parent.[34] Similarly, New Hampshire requires parents to consent to any "non-academic survey or questionnaire,"[35] and West Virginia prohibits the collection of whether a student and their family "were recipients of financial assistance from a state or federal agency."[36]

Sharing Student Data with Third Parties Such as Broadband and Device Providers

Schools may choose to share data they collect with broadband and device providers to provide connectivity, devices, or services,[37] to administer or implement a broadband or device program more efficiently,[38] to ensure that the program is using public resources responsibly,[39] or to conduct research. For example, in Wisconsin, the Department of Public Instruction collected data on students' broadband needs through a survey and then shared that data with broadband providers to obtain service information for specific student addresses.[40] That data sharing, however, occurred only after the Department of Public Instruction established data sharing agreements between broadband providers and schools.[41]

Privacy and Equity Risks

Although sharing data carries benefits for schools, students, and families, it also carries significant risks:

- **Secondary Uses of Data:** Secondary data use occurs when data is re-used for additional purposes beyond the original intended use, potentially diverging from the scope of what the data subject was notified of, expected, or consented to, such as marketing.[42]
- **Lack of Meaningful Consent and Loss of Trust:** Sharing of data with broadband and device providers and third parties can pose challenges to meaningful consent and threaten community trust. Families or students may not expect broadband or device providers to receive their data or to repurpose it for secondary uses.
- **Maintaining Direct Control of Shared Data:** Sharing data with external partners presents the risk that the data may be reshared, given less protection from breaches

and security threats, or subject to less stringent data governance practices, such as restrictions on access, retention, and internal use.

- **Legal Risk:** As with data collection, federal, state, and local laws dictate how schools may share student data, and schools may face legal risk in entering partnerships with broadband and device providers to get students connected if schools have not conducted appropriate diligence and do not have proper agreements in place.

Privacy-Forward and Equity-Forward Practices

To meet the challenges that come with sharing data with third parties, schools should deploy the following three practices:

- Develop robust data governance;
- Engage the community; and
- Comply with legal rules, including the Family Educational Rights and Privacy Act (FERPA).

Develop Robust Data Governance

Data governance is even more essential when data is shared across multiple entities, especially with private third-party partners, who may rely on different values and assumptions when dealing with shared data.[43] Schools establishing data sharing programs with broadband or device providers will need to ensure they have appropriate structures and procedures in place to consider whether sharing is appropriate, necessary, and consistent with students' and families' expectations, and develop clear policies that govern the roles, responsibilities, and processes for sharing.

Aspects of data governance may be required by local, state, or federal rules.[44] The following data governance practices and policies will help schools and school districts address the risks related to sharing student data:

- **Data Sharing Agreements:** When sharing student data with third parties, schools should enter into a written data sharing agreement. Those agreements should be tailored to a school's specific sharing needs and typically include items such as:
    - type of information being collected and shared;
    - the permitted and prohibited uses of the information;
    - methods of collection and sharing;
    - retention and destruction of the information shared, including a timeline or conditions for doing so;

    - protocols for addressing a violation of the data sharing agreement or other data incidents such as an unauthorized disclosure due to a breach, including clear roles for partner organizations, responsibilities for providing remedies in the event of a breach, and timely communication with families so they know where to go for assistance; and,
    - limitations on access to and redisclosure of the information.

  Schools and districts also should be aware that state law may require them to develop data sharing agreements with certain elements[45] and that guidance, model contracts, and model data sharing agreements exist.[46] The U.S. Department of Education also provides guidance on data sharing agreements, including a checklist of items to consider as part of the contract.[47]

- **Purpose, Use, and Redisclosure Limitations**: Data shared to get students online may be sensitive, and schools have to retain control over how it is used, or potentially risk exposing students to secondary data uses that harm them. One approach to mitigate this risk is to include purpose, use, and redisclosure limitations in the aforementioned data sharing agreement.[48] Data sharing and use should be limited to educational purposes,[49] which the schools should publicly delineate for their communities. In this case, “educational purposes” would entail data sharing solely to connect students at home to complete their schoolwork. “Educational purposes” must exclude commercial purposes such as marketing without discrete, meaningful parental consent.
- **Data Minimization**: Data sharing should incorporate principles of data minimization. Schools should ensure that they and their partners have policies and technical controls to limit access to only individuals who have a clear need for it to get students connected. Recipients of the data should be limited to those with a “need to know.”
- **Transfer, Storage, and Destruction Plans:** Schools should establish with partners when and how data will be transferred, stored, and destroyed.[50] Schools should use secure transfer methods such as secure file transfers, feeds, and data-sharing services. Insecure methods, such as email or fax, are susceptible to interception and do not provide enough protection for sensitive student information.[51] Schools also should ensure that partners use secure methods for storing data and adhere to the schools’ plans for the data’s eventual destruction.[52]

Engage the Community

To help address concerns about sharing data, schools and their partners should engage diverse groups of stakeholders like students, families, teachers, and administrators not directly involved in the data sharing program. That engagement should help schools determine both how data should be shared with partners and/or whether that sharing should take place at all. Schools should be transparent and disclose what data may be shared with service providers such as broadband companies to help connect students.

To effectively engage communities, engagement should also seek to equitably empower the diverse communities they serve. To do so, education leaders should engage community members proactively and early in the process and build stakeholder capacity for engagement, including by providing them necessary information to respond appropriately.

Comply with Legal Rules

If schools intend to share data with device or broadband providers, schools should ensure they comply with the federal Family Educational Rights and Privacy Act (FERPA).[53] FERPA generally prohibits the disclosure of students' "personally identifiable information" (PII) without parents' consent unless the data sharing meets one of FERPA's exceptions.[54] One exception, which was updated in 2009 to permit sharing with "outside service providers" that are "acting for" the school and meet certain requirements,[55] may be relevant:

- **School Official Exception:** The school official exception permits disclosure of PII without consent to "school officials" who are designated by the school if they meet the following requirements:
    - perform a function "for which the agency or institution would otherwise use employees";
    - have "a legitimate educational interest" in the education records;
    - are "under the direct control" of the school "with respect to the use and maintenance of education records"; and
    - use education records only for authorized purposes and do not redisclose PII from education records to other parties without consent.[56]

  A school using the school official exception must provide parents with a "specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest" in its annual notice of FERPA rights.[57] Although a written information sharing agreement is not required under the school official exception, it is a best practice for schools to establish one.[58] Conversely, a data sharing agreement alone does not qualify for the school official exception, unless all of the exception's requirements are met.

Another FERPA exception that arises but is unlikely to support data sharing needed to connect students, is the "directory information" exception. "Directory information" is student data that, according to FERPA, would generally be considered "harmless" if released and could include a student’s name and address.[59] However, this information may be disclosed without parental consent only if (1) the school has provided notice to parents of the PII it has designated as directory information, and (2) parents have not opted out of its disclosure.[60] Given these two requirements, a broadband or device provider would be unlikely to receive complete individual-level student data from schools, thus undercutting their ability to rely on that data for purposes of identifying *all* students’ needs. Additionally, addresses that are expressly or implicitly tied to other, non-directory information such as a student's need for broadband may not qualify as directory information.[61]

Monitoring Student Activity Online

Schools have long monitored and coached students on their use of computers and the internet.[62] Twenty years ago, that monitoring took place in-person, with direct supervision of students’ and communities’ use of computer labs located on school campuses.[63] However, with the advent of new technologies, the possibilities of remote learning have expanded dramatically,[64] and the COVID-19 pandemic has made remote learning a necessity for many students.

With those new technologies and the expansion of remote learning, schools have increasingly deployed technically sophisticated means of monitoring students’ online activity.[65] Monitoring technology is used to manage school-issued devices remotely and monitor student activity on the internet, both at school and at home. Monitoring technology goes beyond the data collection and sharing necessary to get students connected and may permit teachers, administrators, and other school staff to see what students have open on their computer screens, open websites on a student’s laptop, switch tabs, block sites, access communications, or view browsing histories. Security flaws have also permitted school personnel to access students’ cameras and microphones without students’ permission or awareness.[66]

School administrators that use monitoring software have stated that they seek to accomplish goals like protecting student safety,[67] supporting student engagement,[68] and/or complying with legal requirements, such as the federal Children’s Internet Protection Act (CIPA).[69] All of these objectives are important to achieving positive educational outcomes; nonetheless, monitoring technology has been controversial.

For example, in Minneapolis schools, parents pushed back against the district’s use of algorithmic software to monitor students online.[70] The software uses algorithmic technology to “scan billions of student emails, chat messages and files each year in search of references to sex, drugs and violence.”[71] According to school administrators, the software is a valuable tool to protect students, but in addition to searching for words such as “gun” or “kill me,” it also disproportionately flags “LGBTQ-specific words.”[72]

The Harms of Monitoring Student Activity Online

Systems for monitoring students’ online activities are gaining popularity in K-12 education settings.[73] Some schools and school districts are turning to student activity monitoring technology as a response to the threat of mass shootings and concerns about student safety.[74] Companies market their monitoring technologies with claims that they can identify sexual content and drug and alcohol use; prevent mass violence, self-harm, and bullying; and/or flag students who may be struggling with academic or mental health issues and need help.[75] There is limited comprehensive data, but available figures, as well as statements from the companies themselves, suggest that spending by U.S. school districts on monitoring tools has risen substantially in recent years.[76] However, the claims of effectiveness by companies selling these products are largely unproven,[77] and these tools can endanger the very students they are supposed to protect. Surveilling students’ online activities raises serious privacy, free expression, and other civil and human rights concerns that schools, districts, and legislatures should safeguard against.[78]

From a privacy standpoint, systematic monitoring of online activity can reveal sensitive information about a student’s personal life, such as their sexual orientation or health information. Additionally, surveilling students online can cause a “chilling effect” on students’ speech, dissuading them from expressing their views, engaging in political organizing, or discussing sensitive issues such as mental health.[79] And these and other risks of harm from monitoring are likely to be disproportionately borne by minority or marginalized communities, including students of color, immigrants, and Muslim students or other religious minorities.[80] These groups may face a higher risk of punishment or law enforcement contact based on monitoring[81] and may be particularly chilled for fear of punishment.[82]

Because of the threat to equity, student privacy, and free expression, if schools chose to monitor students’ online, they should adopt a community-centered approach which should be limited to only minimal data access and collection.

Privacy and Equity Risks

The monitoring technologies adopted by some schools are broad and operate at all levels of students' online experience, including on school-issued devices, on school networks, through web apps, and even by "force installing"[83] browser extensions. This surveillance can harm students in multiple ways:

- **Invasion of Privacy and Loss of Trust**: Invasive or unexpected monitoring can invade students' privacy, discourage them from using the provided devices, and jeopardize public trust in institutions such as schools that are stewards of student data.[84]
- **Increased Inequities:** Marginalized student populations are often subjected to disproportionate surveillance, due to biases in data or algorithms used to monitor students, power dynamics between schools and students, or a lack of training on the proper uses and limitations of monitoring tools.[85] For example, certain scanning algorithms disproportionately flag words relating to LGBTQ+ students' experiences as problematic,[86] and social media monitoring employed by some schools has been demonstrated to disproportionately flag posts by students of color for review.[87]
- **Chilling Expressive Activities:** Reports show that online surveillance stifles expressive activities.[88] Because online monitoring of student activity is targeted at surveilling students' speech, communications, and online reading, it risks dissuading students from expressing themselves or learning about potentially controversial topics, particularly when it comes to minority views or unpopular opinions.
- **Overcollection and Misuse of Data, Including in Students' Homes**: Overcollection of data can increase risks that the data will be used out of context or disclosed in a data breach.[89] Overcollection can occur through overbroad surveillance, including by hearing family conversations or seeing video of activities in the home. Further, video into students' home lives has resulted in baseless discipline of students, including Black students.[90] Students of color, students with disabilities, and English language learners are already subject to disproportionately high rates of suspension, expulsion, seclusion, and physical restraint, and concerns have emerged that new avenues of technological discipline will follow existing disparities in schools' discipline practices.[91]
- **Loss of Direct Control of Shared Data:** As with any data sharing, monitoring of student activity online presents the risk that the data may be reshared,[92] disclosed in a breach,[93] or subject to less stringent data governance practices, such as restrictions on access and internal use.
- **Wasted Resources and Deterring Participation in Funding Programs**: The use of monitoring and surveillance software redirects schools' limited funds away from other priorities. Some school officials have stated that they (incorrectly) believe invasive

surveillance is required by CIPA, as described in this topic's *Comply with Legal Rules* section.[94]

Privacy-Forward and Equity-Forward Practices

To address harms of monitoring student activity online, schools should seek to limit overbroad monitoring of students' activity online through the following practices:

- Promote equity;
- Engage the community;
- Develop robust data governance practices;
- Build stakeholder capacity and digital literacy; and
- Comply with legal rules, including by understanding the limited requirements of the Children's Internet Protection Act.

Promote Equity

Schools are responsible for ensuring equitable use of data, which includes minimizing bias, addressing power imbalances, using data to highlight existing inequities, and ensuring equitable access to data and technology.[95] Many monitoring technologies use algorithmic software, such as systems designed to scan student messages for signs of self-harm or bullying, and schools should take steps to fully consider whether those technologies are needed or helpful and ensure that those algorithmic technologies do not exacerbate existing inequities:

- **Ground Student Activity Monitoring in What Schools Are Positioned to Address:** Before monitoring student activity, especially using algorithmic software, schools should identify their goals in doing so and determine whether monitoring technology is necessary to or capable of meeting those goals. Consequently, it is important that schools understand the technology's intended domain, which may be quite limited.[96]
- **Balance Urgency to Act with Need for Evidence About What Works**: Schools and districts should look for solutions that have a proven track record of improving school safety and students' wellbeing. Many current trends in data and technology for school safety are experimental and lack evidence to support claims related to student safety. While appropriately tailored and thoughtful data collection can be part of a holistic program to help address students' needs, more data is not necessarily better.[97]
- **Examine Input Data for Bias:** Ensure that any data used by the monitoring system (for example, lists of approved or banned search terms and websites) is evaluated for bias,[98] because using biased data will produce biased results. One of the concerns with

monitoring software, for example, is that it can disproportionately subject LGBTQ+ students to monitoring because the words “lesbian” and “gay” are flagged as potentially bullying terminology.[99]

- **Govern Appropriate Uses of Software Systems:** Because many systems are effective only in the specific domain they were designed for — and even then may have limitations school officials should be aware of and account for — it is important to document the use cases for the system so it is not used in unintended ways. School officials should seek to understand whether monitoring software was designed for the school setting and to avoid inaccurate or harmful results. Similarly, it is important that algorithmic monitoring systems include basic due process protections such as permitting humans to review algorithmic decisions and to intercede before a student is harmed, and that students and families have access to redress for decisions that interfere with their rights, ability to learn, or educational opportunities.

Engage the Community

Schools should engage communities when deciding whether to implement monitoring software and throughout the implementation process. Engaging stakeholders such as students, families, teachers, and administrators helps ensure any concerns about the system are raised and addressed before the system is put into use.[100] Policymakers and education officials should affirmatively reach out to and engage underrepresented communities, particularly students and families of color, LGBTQ+ students, and students who rely on school-issued devices and connections, who may be disproportionately impacted by the monitoring of online activity. In those efforts, schools should accommodate the diverse communities they serve, including parents that may speak a language other than English, have a disability, or lack access to transportation or broadband internet. Similarly, engagement efforts should provide sufficient information to families and the community to meaningfully evaluate the proposed technology and data use and engage the school’s decision-making and data governance processes.

Develop Robust Data Governance

Schools should ensure that they have data governance procedures and processes in place for any monitoring of students’ activity online, including establishing how data is stored, shared, and governed and how to minimize the data that is collected:

- **Purpose, Use, Access, and Redisclosure Limitations.** As monitoring software collects data on students, it raises similar data governance concerns as data shared with broadband and device providers. Schools should ensure they have appropriate data governance structures and data sharing agreements with monitoring companies to establish purpose, use, access, and redisclosure limitations, as well as requirements for the secure transfer, storage, and destruction of data. Purpose and use limitations should restrict technology to educational purposes and exclude commercial or marketing purposes — even if the technology is free. Standards for developing these limitations responsibly can be found in CDT's recent guidance on data ethics.[101]

- **Data Minimization.** Data governance also includes data minimization. For example, schools should collect only aggregate information whenever possible, such as trend analysis of security threats or identification of problematic sites that are being accessed by multiple students. Schools should also minimize where monitoring is occurring, such as by monitoring aggregate traffic on the school network, rather than over individual devices, to identify unauthorized access or activity.[102] Further, schools should not be permitted to remotely enable and monitor device cameras and microphones, which foreseeably would capture private family conversations and activities inside the home, without meaningful and explicit parental consent.[103] Schools should have a plan in place for destroying data collected by monitoring technology, as described in this topic's *Using Data to Assess Needs and Launch Connectivity and Device Programs* section.

Build Stakeholder Capacity and Digital Literacy

A report from the Quello Center at the University of Michigan found that students without home internet access or who relied on a cell phone for home internet had significantly lower digital skills than those with home internet access, where "digital skills" included understanding of security and privacy issues like malware, phishing, and privacy settings.[104] For organizations to ethically use data and technology — including monitoring of students' online activity — staff, parents, and other stakeholders must have a clear understanding of the technology, the data it uses and collects, and its purposes, and access to technical support so they can address potential issues that may arise.[105] Schools can increase stakeholder capacity by taking the following actions:

- Equip staff, parents, and other key stakeholders with information to understand how data is collected and used, how bias may occur in algorithmic systems,[106] and how to minimize associated risks of overcollection;
- Provide customized training dependent on individuals' roles and prior knowledge;
- Create documented policies and procedures, and share them publicly to communicate the organization's approach[107];
- Provide regular follow-up trainings, both to refresh knowledge and discuss new developments; and,

- Provide oversight and accountability to ensure that implementation is occurring and not forgotten once the training is completed.[108]

Comply with Legal Rules

Some schools have stated that they believe that invasive monitoring of students' activity online is required by CIPA.[109] CIPA requires schools that participate in the Federal Communications Commission's E-Rate program comply with specific internet safety requirements, including that schools "monitor[] the online activities of minors."[110] CIPA's "monitoring" requirement, however, is not defined, and schools should seek to meet its requirements with narrow, community-centered efforts that are limited to the minimal amount of data collection needed to achieve CIPA's goals, both on- and off-campus.

Using CIPA to justify overly broad surveillance and monitoring of student activity can lead to an extensive list of privacy harms and can be exacerbated when monitoring occurs on devices and services used off-campus, invading students' and families' homes.[111] During debate over CIPA, Senator Patrick Leahy envisioned that "many schools and libraries put their screens in the main reading room. One has to assume not too many kids are going to go pulling up inappropriate things on the web sites when their teachers, their parents, and everybody else are walking back and forth and looking over their shoulder saying: What are you looking at?"[112] Instead of scanning students' messages or actively monitoring their open applications or browser tabs, schools should engage parents and community members to monitor students' online activities and coach them on digital literacy and online citizenship.[113]

Ongoing Security and Device Management Requirements

Distributing devices to students can be an important component of closing the homework gap. However, it also comes with an added responsibility to minimize the potential for harm that can come with those devices, as they can be a vector for attacks on student privacy. In a New Orleans school district, for instance, staff threw computers away without properly destroying data on the computers. They were then found, and the finder was able to access student and school data that had been left on the computers.[114] Consequently, ensuring the devices themselves are as secure as possible, and that there is a governance program in place to enable proper management of devices is critical to protecting student privacy.

Privacy and Equity Risks

Schools and districts should consider the following risks when implementing technical programs to address the homework gap:

- **Ongoing Resource Commitment:** Closing the homework gap requires not just a one-time cost to provide devices and connectivity to students, but ongoing management and replacement costs.[115] That investment of resources into managing devices and connections may divert resources from other priorities.
- **Collecting Data to Track Devices and Connections:** Schools may wish to track which devices and connections are being used by students to identify those in need of support. Such tracking may pose risks to student privacy, especially where the tracking includes accessibility devices for students with disabilities (for instance, keeping track of which students have been issued technology like eye trackers or voice-to-text software). While tracking this data may be necessary, such sensitive information requires robust data governance and security practices.
- **Properly Destroying Data When Retiring Devices:** When retiring devices from educational use, schools must ensure that student data is properly destroyed, including any device backups maintained by the school for convenience or as part of a tracking or monitoring system. This applies whether the devices are disposed of, sold, or donated.

Privacy-Forward and Equity-Forward Practices

Schools may address the privacy risks from ongoing device and connectivity management through two practices:

- Build stakeholder capacity and digital literacy; and
- Implement technical best practices.

Build Stakeholder Capacity and Digital Literacy

Building the skills of all stakeholders, especially those students and families who are inexperienced with technology, can help them manage their school-issued devices in a secure way. Specific supports for students and families will be discussed in the next section, but there are also internal frameworks schools can build to support this development in their communities:

- **Understand Parents' and Students' Technical Needs:** In any use of data or technology, schools should proactively communicate with stakeholders, including families and students. In that communication, schools should seek to understand the families' needs, including for technical support. Schools also should give all users the information they need to operate their school-issued devices in a secure manner and provide ample access to technical support.[116]

- **Provide Training for IT Staff and Educators:** The shift to remote learning not only altered the work of educators[117] but also of technology and privacy practitioners in K-12 education as technical and cybersecurity challenges surged.[118] Training educators and IT staff is a key component of protecting against and responding to data incidents,[119] and schools should prepare them to navigate continued online learning.

Implement Technical Best Practices

Several technical best practices can help keep students, and by extension the broader school community, safe:

- **Manage Access and Roles:** Restrict roles and account access so that users have only the precise level[120] of access they need and no more — known as a *least-privilege* approach. This can limit the avenues of attack for malicious actors and minimize the impact of any mistakes users might make. This is particularly critical for student devices as schools may have different types of concerns and levels of trust in non-employees, such as students and parents, than they do with their own staff and faculty.
- **Keep Software Up to Date:** Automatic or mandatory software updates can keep students safe by ensuring that they always have the latest security patches available for their systems. Many users do not install system updates due to inconvenience or because they are simply unaware that they should do so. Setting up school-issued devices to update automatically avoids requiring users to manage this aspect of security on their own.
- **Offer Technical Support:** Offering technical support to families is a key way to strengthen security, as it gives families the support they need to make security-minded decisions when they are unsure, rather than trying to make their best guess with limited knowledge. One convenient way to offer technical support is by setting up school-issued devices to allow IT staff to access them remotely, relieving users of security management issues by allowing IT staff to handle them directly, which may be the easiest option for large schools and districts with a strong technical and security infrastructure. However, for smaller or less technically mature schools, remote access can be a significant threat vector in its own right.[121] If malicious actors are able to hijack the access, they can do significant harm by snooping around on user devices and abusing their access to school systems. Consequently, these schools should use safer approaches to technical support such as by-appointment office hours or a dedicated help line.

- **Follow Best Practices for Data Destruction:** In addition to supporting students and families while they are using school-issued devices, it is equally important to ensure that those populations, as well as future users of the devices, are protected after the devices have been returned to the school. This means following protocols for destroying any existing data left by the previous user and ensuring that if that device is passed on to a new user, the former user no longer has any sort of access to the device or the information on it. These protocols should include information such as what destruction techniques should be used and what, if any, data should be archived and retained. More information about these protocols can be found in CDT's issue brief on data destruction in education.[122] Additionally, schools should have a plan for retiring devices as they become obsolete. Devices that are no longer supported by their manufacturers with security updates should be retired as soon as possible. Additionally, devices that are unable to run school programs efficiently should be retired so as to not put the students using them at a disadvantage.

Lack of Digital Literacy and Security Knowledge

In addition to managing the technical aspects of security and safety, it is important to give students and families, especially those new to the technical world, the tools they need to keep themselves safe in the digital space. As mentioned above, capacity building within schools and districts is important, but it is also important to build digital literacy in students and families as well.

Privacy and Equity Risks

Closing the homework gap while protecting privacy is not just about devices and internet connectivity but also involves ensuring that technology users, new and old, are equipped to use these new resources safely and securely and have sufficient training and support to feel comfortable bringing technology into their home. Building stakeholder capacity can help address privacy and equity risks such as:

- **Lack of Technical Capacity:** Human error plays a role in up to 95 percent of data incidents, including opening infected attachments or clicking unsafe links.[123] Students and families may lack the digital skills and experience necessary to navigate those security challenges.[124] Training stakeholders on how to prevent these incidents is critical, particularly when these devices are in family homes, exposing users to all the attendant security risks.

- **Misuse of Technology**: Any new technology program should first be grounded in the purpose it is intended to serve. In the case of the homework gap, it should be made clear what the appropriate, education-focused uses are and what are unsafe or inappropriate uses. Many schools cover this in acceptable use policies, but it is important that this information is grounded in why it matters, and the related guidance and expectations are made clear to students and families. Additionally, those policies should account for the reality of their students' lives. In some cases, multiple family members may use a student's device without their knowledge and may violate a school's appropriate use policy, causing a disproportionate impact or disciplinary action on some students and families who do not have access to multiple devices within the home. If the school-provided technology is something such as broadband access or a mobile hotspot, it may be overly restrictive to try to manage what students or families are using the device for if that is their primary or only internet connection, to the extent permitted by local, state, and federal rules.[125] Policies should account for and address use cases like these.
- **Disproportionate Impact on Some Students and Families**: While the use of school-issued devices carries some associated risks for all students and families, adjusting to the devices may place disproportionate strain on families that have less experience using these technologies. They may need to do more work to figure out how to use the devices and, if devices are only given to families on an as-needed basis, some families may be using older, less sophisticated, or lower-quality devices than others. In some cases, this may mean the device itself is less secure or requires more effort from the user to be operated in a secure way. Additionally, users and families with more limited access and thus less technical experience may be more likely to expose themselves to harm via unsafe security practices and may be less aware of what data they are sharing, as suggested by recent research from the Quello Center.[126]

Privacy-Forward and Equity-Forward Practices

To address these inequities, it is important to give students and families the training and information they need to use their new devices safely.[127] It is also important to provide support hotlines, troubleshooting office hours, recurring educational workshops, etc. to ensure that users know how to take advantage of privacy protections. Specifically, education leaders should focus on building digital literacy and security knowledge through these practices:

- Build stakeholder capacity and digital literacy by providing security and safety training;
- Engage the community; and

- Develop robust data governance by setting privacy-forward policies.

Build Stakeholder Capacity and Digital Literacy

Students, families, and teachers should be provided with training about safely using devices to interact with services online, especially when those systems may be unfamiliar. In particular, it may be useful to train users on the "operational security" aspects of maintaining security and privacy, since these may be unintuitive to many users.

- **Teach Students and Families to Implement Best Practices:** As the stewards of the devices, students and families play a key role in maintaining their security. The next section discusses some of the technical best practices that can help keep student devices secure, but many of these practices may not be intuitive to students and families. For instance, keeping software up to date may seem like more of a convenience than a security practice, but it is a key component of device security. Schools should provide training and information about best practices when they give devices to students. Schools also should help build a culture of security by setting up frameworks for long-term support and assistance to students. This means ensuring students and families have a point of contact for tech support and security questions and may also mean setting up targeted training sessions for recurrent issues.
- **Human Factors in Security:** Operational security is the practice of protecting systems against attacks that do not rely on software or hardware vulnerabilities, but rather on manipulating users or taking advantage of mistakes. Tactics may include:
    - gleaning information like passwords by observing people when they are using their devices in public or insecure places (also known as "shoulder surfing");
    - taking advantage of weak or reused passwords;
    - gaining access to systems by social engineering[128] (using people's natural social impulses against them, such as an attacker asking for the school Wi-Fi password because "they forgot," when in practice they are trying to access the network for malicious reasons); and
    - Tactics such as phishing (sending emails or messages trying to get users to click on malicious links).

  These attacks can often be prevented by users who are aware of them and given the tools to spot them.
- **Maintain Secure Password Practices:** As mentioned above, passwords are a critical component of keeping accounts and information secure. Students should be required or strongly encouraged to password-protect any school-issued device they are given. School IT staff should maintain a mechanism for resetting passwords if the student loses

or forgets the password they have chosen for their device. Where possible, it may make sense for schools to support this through policy (such as using a single-sign-on system for school accounts to avoid password reuse). However, schools should also teach students and families what makes a secure password (such as, not using common words or easily discoverable personal information) so that users can carry that knowledge over to other systems and environments.

- **Safety**: For novice users, especially children, more basic training about why some information is best kept private and how many safety lessons translate to the digital space may be useful.[129] In much the same way that children learn to be aware of their surroundings in parking lots or sidewalks, they should also apply that same caution to digital environments like the internet.
- **In-Home Security Basics:** For users who are new to in-home internet access, training on secure passwords and the value of using a secure network instead of an insecure one may also be useful. Users may not realize that password protecting a network does more than just keep people from stealing bandwidth — it can also be an important part of protecting other devices using that same network.

Engage the Community

When designing device and digital literacy programs, understanding the concerns and needs of students and families will be critical to garnering the buy-in and comfort that will be critical to the success of the programs. Engagement should make room for families to discuss their concerns and questions about the program and how those concerns might be mitigated, such as by offering alternatives like extended computer lab hours on campus for students who are uncomfortable bringing devices into their homes.

Develop Robust Data Governance

Part of the training on using devices securely should also be to explain the reasoning behind any device usage policies put in place by the school.[130] Ensuring that students and families understand what harm the policies are intended to protect against can be an important component of garnering buy-in to follow those policies more carefully. It can prevent people from searching for convenient workarounds to "inconveniences" like password protecting devices if they understand that the workaround may undermine their safety and that of the rest of the school community.

Conclusion

The pandemic brought the necessity and urgency of closing the digital divide into sharp relief. However, it is also clear that efforts to address the disparity cannot come at the expense of equity and privacy, or they run the risk of further disadvantaging the very students they are meant to help. The practices and considerations laid out in this brief provide a roadmap to addressing the digital divide in a privacy- and equity-forward way to ensure that all students have equal access to education in an increasingly digital world.

[1] Bracey Harris, *Homework in a McDonald's Parking Lot*, Hechinger Report (June 27, 2020), https://hechingerreport.org/homework-in-a-mcdonalds-parking-lot-inside-one-mothers-fight-to-help-her-kids-get-an-education-during-coronavirus.

[2] Emily Nitcher & Joe Dejka, *What Happens if Schools Go Remote This Fall and Many Nebraska Kids Don't Have Internet?*, Omaha World Herald (June 12, 2020), https://omaha.com/news/education/what-happens-if-schools-go-remote-this-fall-and-many-nebraska-kids-dont-have-internet/article_6ad0719f-315d-5c47-b33a-94688432d9d3.html.

[3] Editorial, *Doing Schoolwork in the Parking Lot Is Not a Solution*, N.Y. Times (July 18, 2020), https://www.nytimes.com/2020/07/18/opinion/sunday/broadband-internet-access-civil-rights.html.

[4] Jessica Fregni, *How Rural Students Are Left Behind in the Digital Age*, Teach for America (Jan. 17, 2020), https://www.teachforamerica.org/stories/how-rural-students-are-left-behind-in-the-digital-age.

[5] *Inquiry Concerning Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion*, Fourteenth Broadband Deployment Report, GN Docket No. 20-269, 36 FCC Rcd 836, 865-66, para. 46 (2021), *available at* https://www.fcc.gov/document/fcc-annual-broadband-report-shows-digital-divide-rapidly-closing (percent of households throughout the United States with fixed terrestrial broadband of at least 25/3 Mpbs).

[6] Common Sense et al., *Looking Back, Looking Forward* 10 (2021), *available at* https://www.commonsensemedia.org/sites/default/files/uploads/pdfs/final_-_what_it_will_take_to_permanently_close_the_k-12_digital_divide_vfeb3.pdf

[7] *Id.* at 9.

[8] Monica Anderson & Andrew Perrin, *Nearly One-In-Five Teens Can't Always Finish Their Homework Because of the Digital Divide*, Pew Research Center (Oct. 26, 2020), https://www.pewresearch.org/fact-tank/2018/10/26/nearly-one-in-five-teens-cant-always-finish-their-homework-because-of-the-digital-divide/.

[9] Jason Shueh, *FCC Commissioner to Tech Industry: It's Time to Reinvent Textbooks, Teaching*, Government Technology (Jan. 9, 2015), https://www.govtech.com/education/fcc-commissioner-to-tech-industry-its-time-to-reinvent-textbooks-teaching.html.

[10] Alyson Klein, *Acting FCC Chair: The 'Homework Gap' Is an 'Especially Cruel' Reality During the Pandemic*, Education Week (Mar. 10, 2021), https://www.edweek.org/technology/acting-fcc-chair-the-homework-gap-is-an-especially-cruel-reality-during-the-pandemic/2021/03.

[11] Council of Chief State School Officers, *Home Digital Access Data Collection: Blueprint for State Education Leaders* 3 (2020), *available at* https://digitalbridgek12.org/states/data-collection-blueprint.

[12] Common Sense et al., *Looking Back, Looking Forward*, *supra* note 6, at 9; Connecticut Commission for Educational Technology, *Home Internet Connectivity* 4 (2021), *available at* https://portal.ct.gov/-/media/DAS/CTEdTech/publications/2021/2021_CET_K-12_Winter_Connectivity.pdf.

[13] *Advancing Equitable Internet Access in Connecticut*, Center for Democracy & Technology (Dec. 16, 2020), https://cdt.org/insights/cdt-tech-tales-advancing-equitable-internet-access-in-connecticut/; *see also* Connecticut Commission for Educational Technology, *Home Internet Connectivity*, *supra* note 12, at 4 (survey of schools on barriers faced by families in adopting state-supported broadband).

[14] Venky Anant et al., *The Consumer-Data Opportunity and the Privacy Imperative*, McKinsey & Co. (Apr. 27, 2020), https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (finding that half of consumers "are more likely to trust a company that asks only for information relevant to its products or that limits the amount of personal information requested").

[15] Corey Chatis, Missy Cochenour & Stephanie Irvine, SLDS Grant Program, National Center for Education Statistics, *Early Childhood Data Governance in Action!*, *available at* https://nces.ed.gov/programs/slds/pdf/EC_DataGovernance_Initial.pdf.

[16] Corey Chatis & Kathy Gosa, SLDS Grant Program, National Center for Education Statistics, *Considerations for Collecting New Data Elements* 1-2 (2016), *available at* https://slds.ed.gov/services/PDCService.svc/GetPDCDocumentFile?fileId=18636.

[17] Connecticut Commission for Educational Technology, *Home Internet Connectivity*, *supra* note 12, at 4; *Advancing Equitable Internet Access in Connecticut*, Center for Democracy & Technology, *supra* note 13.

[18] Elizabeth Laird & Cody Venzke, Center for Democracy & Technology, *Comments for the Advisory Committee on Data for Evidence Building* 2 (2021), *available at* https://cdt.org/insights/cdts-comments-for-the-advisory-committee-on-data-for-evidence-building/.

[19] Data should also be encrypted when in transit, discussed in more depth in the section on sharing student data.

[20] Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Balancing the Scale of Student Data Deletion and Retention in Education* (2019), *available at* https://cdt.org/insights/report-balancing-the-scale-of-student-data-deletion-and-retention-in-education/.

[21] Privacy Technical Assistance Center, *Data Breach Response Checklist* (2012), *available at* https://studentprivacy.ed.gov/resources/data-breach-response-checklist.

[22] *See* Daniel Castro and Travis Korte, *Parents and Educators Should Embrace, Not Fear Student Data*, Center for Data Innovation (Dec. 3, 2013), https://datainnovation.org/2013/12/parents-and-educators-should-embrace-not-fear-student-data/.

[23] Elizabeth Laird, *Responsible Use of Data and Technology in Education: Community Engagement to Ensure Students and Families Are Helped, Not Hurt*, Center for Democracy & Technology (Feb 22, 2021), https://cdt.org/insights/responsible-use-of-data-and-technology-in-education-community-engagement-to-ensure-students-and-families-are-helped-not-hurt/.

[24] Elizabeth Laird, Center for Democracy & Technology, *Responsible Use of Data and Technology in Education* 2 (2021), *available at* https://cdt.org/insights/responsible-use-of-data-and-technology-in-education-community-engagement-to-ensure-students-and-families-are-helped-not-hurt/.

[25] Privacy Technical Assistance Center, *Guidance for Reasonable Methods and Written Agreements* at 8 (Aug. 2015), https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements.

[26] For guidance on the PPRA and the federal Family Educational Rights and Privacy Act (FERPA), see Student Privacy Policy Office, U.S. Department of Education, *Protecting Student Privacy*, https://studentprivacy.ed.gov/ (last visited May 12, 2020).

[27] 20 U.S.C. § 1232h.

[28] *Id.* § 1232h(b), (c)(1)(B). The PPRA also applies to surveys of a student's or family's political affiliations or beliefs, mental or psychological problems, sexual behaviors or attitudes, "illegal, anti-social, self-incriminating, or demeaning behavior," "critical appraisals of others," legally recognized privileged relationships, and religious practices, affiliations, or beliefs.

[29] 20 U.S.C. § 1232h(c)(1)(B), (c)(2)(C); Student Privacy Policy Office, U.S. Department of Education, *Protection of Pupil Rights Amendment (PPRA) General Guidance* 1 (2020), *available at* https://studentprivacy.ed.gov/resources/protection-pupil-rights-amendment-ppra-general-guidance.

[30] 20 U.S.C. § 1232h(b).

[31] 20 U.S.C. § 1232h(c)(1)(B) ("including the right of a parent of a student to inspect, upon the request of the parent, any survey containing one or more of such items"). The PPRA also permits parents to inspect surveys created by a "third party," regardless of whether it covers the statute's list of protected topics. *Id.* § 1232h(c)(1)(A)(i).

[32] *See State Student Privacy Laws*, Student Privacy Compass, https://studentprivacycompass.org/state-laws/ (last visited Mar. 29, 2021).

[33] Mark Lieberman, *Knowing How Students and Teachers Use Tech Is Vital*, Education Week (July 22, 2020), https://www.edweek.org/technology/knowing-how-students-and-teachers-use-tech-is-vital/2020/07 (school

districts using low login rates as a proxy for lack of broadband connectivity); Hannah Natanson, *Schools Are Some Families' Best Hope for Internet Access, But Virginia Laws Are Getting In the Way*, Washington Post (May 26, 2020), https://www.washingtonpost.com/local/education/schools-are-some-families-best-hope-for-internet-access-but-virginia-laws-are-getting-in-the-way/2020/05/22/520cc46c-95f3-11ea-82b4-c8db161ff6e5_story.html ("By analyzing activity on student devices in early March, Arlington officials identified roughly 1,000 households without connectivity . . . .")

[34] La. Rev. Stat. § 17:3914(C)(1)(k)-(*l*).

[35] N.H. Rev. Stat. § 186:11 IX-d.

[36] W. Va. Code § 18-2-5(b)(11), (c)(9).

[37] *An Introduction to Sponsored Service*, EducationSuperHighway, https://www.educationsuperhighway.org/a-guide-to-sponsored-service/ (last visited Apr. 19, 2021) (describing uses of student address data to identify possible broadband providers).

[38] *See How North Dakota Bridged the COVID-19 Home Access Gap*, Digital Bridge K-12, https://digitalbridgek12.org/states/how-north-dakota-bridged-the-home-access-gap/ (last visited Mar. 29, 2021).

[39] *See Emergency Broadband Benefit Program*, WC Docket No. 20-445, Report & Order, FCC 21-29 at 34, para. 68 (Feb. 26, 2021), *available at* https://www.fcc.gov/document/fcc-adopts-report-and-order-emergency-broadband-benefit-program-0 (*EBBP Order*).

[40] *Cooperation and Community Engagement at the Wisconsin Department of Public Instruction*, Center for Democracy & Technology (Dec. 16, 2020), https://cdt.org/insights/cdt-tech-tales-cooperation-and-community-engagement-at-the-wisconsin-department-of-public-instruction/.

[41] *Digital Learning Bridge*, CESApurchasing, https://cesapurchasing.org/digital (last visited Apr. 12, 2021).

[42] *See, e.g.*, *FCC Proposes Over $200M in Fines for Wireless Location Data Violations*, Federal Communications Commission (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations; Steve Augustino, *Verizon Agrees to Pay $7.4 Million to Resolve CPNI Investigation*, Commlaw Monitor (Sept. 5, 2014), https://www.commlawmonitor.com/2014/09/articles/privacy/verizon-must-pay-7-4-million-for-misuse-of-cpni/ (describing "Verizon's use of customers' subscription and call information to market new services").

[43] John Fantuzzo et al., *The Integrated Data System Approach: A Vehicle to More Effective and Efficient Data-Driven Solutions in Government* 18 (2017), *available at* https://www.aisp.upenn.edu/wp-content/uploads/2017/09/The-IDS-Approach_Fantuzzo-et-al.-2017_Final.pdf.

[44] *See, e.g.*, Colo. Rev. Stat. § 22-16-104; Idaho Code Ann. § 33-133(3); Mo. Rev. Stat. § 161.096.

[45] *See, e.g.*, Colo. Rev. Stat. § 22-16-107; Idaho Code Ann. § 33-133(7); Mo. Rev. Stat. § 161.096(2)(a)(d).

[46] *E.g.*, *SDPC Resource Registry*, A4L https://privacy.a4l.org/sdpc-resource-registry/ (last visited May 4, 2021); *Sample Privacy and Security Policies*, Colorado Department of Education (May 7, 2018), https://www.cde.state.co.us/dataprivacyandsecurity/sampleitpolicies; *see also* Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Data Sharing & Privacy Demands in Education* (2019), *available at* https://cdt.org/insights/data-sharing-privacy-demands-in-education-how-to-protect-students-while-satisfying-policy-legal-requirements/.

[47] *See* Privacy Technical Assistance Center, *Guidance for Reasonable Methods and Written Agreements* (2015), *available at* https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements; Privacy Technical Assistance Center, *Written Agreement Checklist* (July 2015), *available at* https://studentprivacy.ed.gov/resources/written-agreement-checklist.

[48] *See* Center for Democracy & Technology et al., *Principles for Protecting Civil Rights and Privacy During the COVID-19 Crisis* 2-3 (June 12, 2020) *available at* https://cdt.org/insights/cdt-joins-principles-for-protecting-civil-rights-and-privacy-during-the-covid-19-crisis.

[49] White House Big Data and Privacy Working Group, *Big Data: Seizing Opportunities, Preserving Values* 2 (2015), *available at* https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf.

[50] Laird & Venzke, *Data for Evidence Building*, *supra* note 18, at 2.

[51] Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Protecting Student Privacy While Supporting Students Who Change Schools* 11 (2019), *available at* https://cdt.org/wp-content/uploads/2019/07/2019-06-20-Portability-and-Privacy-Issue-Brief.pdf.

[52] *See generally*, Laird & Quay-de la Vallee, *Data Deletion*, *supra* note 20.

[53] 20 U.S.C. § 1232g. Other laws such as the PPRA, 20 U.S.C. § 1232h, the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06, and state laws may apply as well.

[54] 34 C.F.R. § 99.30.

[55] Family Educational Rights and Privacy, Office of Planning, Evaluation, and Policy Development, Department of Education, 73 Fed. Reg. 74805, 74814 (Dec. 9, 2008), *available at* https://www.federalregister.gov/documents/2008/12/09/E8-28864/family-educational-rights-and-privacy.

[56] *Id.* § 99.31(a)(1); Privacy Technical Assistance Center, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* 4 (2014), *available at* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf.

[57] 34 CFR § 99.7(a)(3)(iii).

[58] Student Privacy Policy Office, *Must a School Have a Written Agreement or Contract With a Community-Based Organization to Which it Non-Consensually Discloses Education Records to Outsource an Institutional Service Under the School Official Exception?*, Protecting Student Privacy, https://studentprivacy.ed.gov/faq/must-school-have-written-agreement-or-contract-community-based-organization-which-it-non (last visited Apr. 20, 2021).

[59] 34 C.F.R. § 99.3 ("Directory information includes, but is not limited to, the student's name; address . . . ."); *see also* Student Privacy Policy Office, U.S. Department of Education, *Model Notice for Directory Information* (2011), *available at* https://studentprivacy.ed.gov/node/428 (designating name and address, among other things, as directory information).

[60] 34 C.F.R. § 99.37(a)-(b).

[61] *See* Letter from LeRoy Rooker, Director, Family Policy Compliance Office, to Lourdes Barro, Associate Executive Director, Phi Kappa Phi (Aug. 28, 2008), *available at* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/LettertoPhiKappaPhiRegardingDirectoryInformationAugust2008.pdf ("Generally, a student's directory information that is linked to other, non-directory information, such as the student's grades, cannot be disclosed absent consent.").

[62] 146 Cong. Rec 5845-73 (daily ed. June 27, 2000) (statement of Sen. Leahy), *available at* https://www.congress.gov/congressional-record/2000/06/27/senate-section/article/S5845-2 ("[N]ot too many children [] are going to be downloading wild, offensive things when they know their parents, their teachers, and the librarians are going to be walking back and forth and seeing it.")

[63] *Schools and Libraries Universal Service Support Mechanism*, CC Docket No. 02-6, Sixth Report & Order, 25 FCC Rcd 18762, 18783, para. 41 (Sept. 28, 2010), *available at* https://www.fcc.gov/document/schools-and-libraries-universal-service-support-mechanism-national (*2010 E-Rate Order*); *id.* at 18775, para. 25 ("[A]ny community use of E-rate funded services at a school facility shall be limited to non-operating hours of the school and to community members who access the Internet while on a school's campus.").

[64] *2010 E-Rate Order*, 25 FCC Rcd at 18783, para. 42.

[65] Dian Schaffhauser, *K–12 Data Privacy During a Pandemic*, T.H.E. Journal (Sept. 10, 2020), https://thejournal.com/Articles/2020/09/10/K12-Data-Privacy-During-a-Pandemic.aspx.

[66] Nader Issa, *CPS Teachers Could Look Inside Students' Homes — Without Their Knowledge — Before Fix*, Chicago Sun Times (Oct 5, 2020), https://chicago.suntimes.com/education/2020/10/5/21497946/cps-public-schools-go-guardian-technology-privacy-remote-learning.

[67] Erica L. Green, *Surge of Student Suicides* Pushes *Las Vegas Schools to Reopen*, N.Y. Times (Jan. 24, 2021), https://www.nytimes.com/2021/01/24/us/politics/student-suicides-nevada-coronavirus.html.

[68] Jordyn Haime, *Remote Learning Progress Report: Keeping Track Of Students In Large Classes Is a Hurdles* [sic], Concord Monitor (Aug. 10, 2020), https://www.concordmonitor.com/Granite-State-News-Collaborative-35623159; Hannah Natanson, *Schools Are Some Families' Best Hope for Internet Access, but Virginia Laws Are Getting in the Way*, Washington Post (May 26, 2020), https://www.washingtonpost.com/local/education/schools-are-some-families-best-hope-for-internet-access-but-virginia-laws-are-getting-in-the-way/2020/05/22/520cc46c-95f3-11ea-82b4-c8db161ff6e5_story.html ("By analyzing activity on student devices in early March, Arlington officials identified roughly 1,000 households without connectivity . . . .").

[69] Mark Keierleber, *Minneapolis School District Addresses Parent Outrage Over New Digital Surveillance Tool as Students Learn Remotely*, The 74 (Oct. 28, 2020), https://www.the74million.org/minneapolis-school-district-addresses-parent-outrage-over-new-digital-surveillance-tool-as-students-learn-remotely.

[70] Mark Keierleber, *'Don't Get Gaggled': Minneapolis School District Spends Big on Student Surveillance Tool, Raising Ire After Terminating Its Police Contract*, The 74 (Oct. 18, 2020), https://www.the74million.org/article/dont-get-gaggled-minneapolis-school-district-spends-big-on-student-surveillance-tool-raising-ire-after-terminating-its-police-contract/.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] Faiza Patel *el al.*, *School Surveillance Zone*, Brennan Center for Justice (Apr. 20, 2019), https://www.brennancenter.org/analysis/school-surveillance-zone; Tom Simonite, *Schools are Mining Students' Social Media Posts for Signs of Trouble*, Wired (Aug. 20, 2018), https://www.wired.com/story/algorithms-monitor-student-social-media-posts/.

[75] Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, The Guardian (Oct. 22, 2019), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle.

[76] Patel *el al.*, *School Surveillance Zone*, *supra* note 74.

[77] Nasser Eledroos & Kade Crockford, *Social Media Monitoring in Boston: Free Speech in the Crosshairs*, Privacy SOS (2018), *available at* https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs; Faiza Patel & Rachel Levinson-Waldman, *Monitoring Kids' Social Media Accounts Won't Prevent the Next School Shooting*, Washington Post (Mar. 5, 2018), *available at* https://www.washingtonpost.com/news/posteverything/wp/2018/03/05/monitoring-kids-social-media-accounts-wont-prevent-the-next-school-shooting/.

[78] Center for Democracy & Technology & Brennan Center, *Technological School Safety Initiatives: Considerations to Protect All Students* (2019), *available at* https://cdt.org/insights/technological-school-safety-initiatives-considerations-to-protect-all-students/.

[79] Jonathon W. Penney, *Whose Speech Is Chilled by Surveillance?*, Slate (July 07, 2017), https://slate.com/technology/2017/07/women-young-people-experience-the-chilling-effects-of-surveillance-at-higher-rates.html.

[80] Natasha Duarte, Emma Llansó & Anna Loup, Center for Democracy & Technology, *Mixed Messages: The Limits of Automated Social Media Content Analysis* 10–11 (Nov. 2017), https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/; Advancement Project, *We Came to Learn: A Call to Action for Police-Free Schools* (Sept. 13, 2018), https://advancementproject.org/wecametolearn/.

[81] Sarah Sparks & Alyson Klein, *Discipline Disparities Grow for Students of Color, New Federal Data Show*, Education Week (Apr. 24, 2018), https://www.edweek.org/ew/articles/2018/04/24/discipline-disparities-grow-for-students-of-color.html.

[82] Sarah Brayne, *Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment*, American Sociological Review (Apr. 4, 2014), https://journals.sagepub.com/doi/10.1177/0003122414530398.

[83] *Initial Deployment of the GoGuardian Extensions*, GoGuardian, https://help.goguardian.com/hc/en-us/articles/360019263771-Installing-GoGuardian-Extensions-for-All-Products-Super-User- (last visited Mar. 30, 2021).

[84] Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Data Ethics in Education & The Social Sector* 8 (2021), *available at* https://cdt.org/insights/report-data-ethics-in-education-and-the-social-sector-what-does-it-mean-and-why-does-it-matter/.

[85] *See* Laird & Quay-de la Vallee, *Data Ethics*, *supra* note 84, at 11-12, 14, 22.

[86] Keierleber, *Don't Get Gaggled*, *supra* note 70*.*

[87] Center for Democracy & Technology & Brennan Center for Justice, *Social Media Monitoring in Schools* 3 (2019), *available at* https://cdt.org/insights/social-media-monitoring-in-k-12-schools-civil-and-human-rights-concerns.

[88] Kaveh Waddell, *How Surveillance Stifles Dissent on the Internet*, Atlantic (Apr. 5, 2019), *available at* https://www.theatlantic.com/technology/archive/2016/04/how-surveillance-mutes-dissent-on-the-internet/476955/.

[89] Laird & Quay-de la Vallee, *Data Ethics*, *supra* note 84, at 9.

[90] *See, e.g.*, Tim Elfrink, *A Teacher Saw a BB Gun in a 9-Year-Old's Room During Online Class. He Faced Expulsion*, Washington Post (Sept. 25 2020), https://www.washingtonpost.com/nation/2020/09/25/louisiana-student-bbgun-expulsion/; Kristie Cattafi, *Edgewater School Called Poolie After Sixth-Grader Had Nerf Gun During Zoom Class*, northjersey.com (Sept. 12, 2020),

https://www.northjersey.com/story/news/bergen/edgewater/2020/09/11/edgewater-nj-police-called-after-student-had-nerf-gun-during-zoom-class/3468499001/; Jaclyn Peiser, *A Black Seventh-Grader Played With a Toy Gun During a Virtual Class. His School Called the Police*, Washington Post (Sept. 8, 2020), https://www.washingtonpost.com/nation/2020/09/08/black-student-suspended-police-toy-gun/.

[91] Civil Rights Data Collection, *Data Snapshot: School Discipline* 1 (2014), *available at* https://www2.ed.gov/about/offices/list/ocr/docs/crdc-discipline-snapshot.pdf.

[92] *See* Naaman Zhou, *CEO of Exam Monitoring Software Proctorio Apologises for Posting Student's Chat Logs on Reddit*, The Guardian (July 1, 2020), https://www.theguardian.com/australia-news/2020/jul/01/ceo-of-exam-monitoring-software-proctorio-apologises-for-posting-students-chat-logs-on-reddit.

[93] *See* Jim Nash, *Data Breach Stirs New University Protests About Proctoring Apps*, Biometric Update (Nov. 3, 2020), https://www.biometricupdate.com/202011/data-breach-stirs-new-university-protests-about-proctoring-apps.

[94] Keierleber, *Parent Outrage*, *supra* note 69.

[95] Andrew Cormack, *A Data Protection Framework for Learning Analytics*, 3 Journal of Learning Analytics 91-106 (2016), *available at* https://learning-analytics.info/index.php/JLA/article/view/4554.

[96] CDT & Brennan Center, *School Safety*, *supra* note 78, at 2.

[97] CDT & Brennan Center, *School Safety*, *supra* note 78, at 2.

[98] Prabhakar Krishnamurthy, *Understanding Data Bias Types*, Towards Data Science (Sept. 11, 2019), https://towardsdatascience.com/survey-d4f168791e57.

[99] Keierleber, *Don't Get Gaggled*, *supra* note 70.

[100] Dillon Reisman, AI Now, *Algorithmic Impact Assessments* 13-14 (2018), *available at* https://ainowinstitute.org/aiareport2018.pdf.

[101] See Laird & Quay-de la Vallee, *Data Ethics*, *supra* note 84.

[102] Cybersecurity & Infrastructure Security Agency (CISA), *Ransomware Guide* 5 (2020), *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf; Readiness and Emergency Management for Schools Technical Assistance Center (REMS TAC), U.S. Department of Education, C*ybersecurity Considerations for K-12 Schools and School Districts* 3 ("To protect their networks and systems as part of overall preparedness program, schools and school districts can . . . [m]onitor network continually to assess the risk from cyber threats.").

[103] *See* Hannah Stern, ACLU of Rhode Island, *Zooming in on Students* 9-11 (2020), *available at* https://riaclu.org/en/news/aclu-report-shows-alarming-lack-privacy-protections-students-engaged-remote-learning.

[104] Keith N. Hampton et al., Quello Center, Michigan State University, *Broadband and Student Performance Gaps* 30-32 (2020), *available at* https://quello.msu.edu/wp-content/uploads/2020/03/Broadband_Gap_Quello_Report_MSU.pdf.

[105] Eddie Copeland, *10 Principles for Public Sector Use of Algorithmic Decision Making*, Nesta (Feb. 20, 2018), https://www.nesta.org.uk/blog/10-principles-for-public-sector-use-of-algorithmic-decision-making.

[106] Iris Palmer, New America, *Choosing a Predictive Analytics Vendor: A Guide for Colleges* (2018), *available at* https://www.newamerica.org/education-policy/reports/choosing-predictive-analytics-vendor-guide/,

[107] National Forum on Education Statistics, *The Forum Guide to Data Ethics* 18-19 (2010), *available at* https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2010801.

[108] *Id.*

[109] Keierleber, *Parent Outrage*, *supra* note 69.

[110] 47 U.S.C. § 254(h)(5)(B)(i).

[111] Silverman v. United States, 365 U.S. 505, 511 (1961); *accord* Griswold v. Connecticut, 381 U.S. 479 (1965).

[112] 146 Cong. Rec S5823-45 (daily ed. June 27, 2000) (statement of Sen. Leahy), *available at* https://www.congress.gov/congressional-record/2000/06/27/senate-section/article/S5823-8.

[113] *See* Section V, *infra*, for more on digital literacy.

[114] Danielle Dreilinger, *New Orleans Students Social Security Numbers Found on Auctioned-Off Laptops*, NOLA.com (July 19, 2019), https://www.nola.com/news/education/article_a3594454-2d40-5331-a752-951ab32af1dd.html.

[115] Common Sense et al., *Looking Back, Looking Forward*, *supra* note 6, at 16-17.

[116] *2021 Digital Equity Recommendations to the Mayor*, Digital Equity in DC Education (Jan. 11, 2021), https://www.digitalequitydced.com/testimony.

[117] *See* Kim Ochs, *Considerations for Distance Learning*, Center for Democracy & Technology (Apr. 14, 2020), https://cdt.org/insights/considerations-for-distance-learning-a-7-point-strategy/; William & Ida Friday Institute for Educational Innovation, *Instructional Design Principles for Remote Teaching and Learning* (Apr. 7, 2021), *available at* https://www.fi.ncsu.edu/resources/instructional-design-principles-for-remote-teaching-and-learning/.

[118] Alyson Klein, *Cyberattacks on Schools Soared During the Pandemic*, Education Week (Mar. 10, 2021), https://www.edweek.org/technology/cyberattacks-on-schools-soared-during-the-pandemic/2021/03; K-12 Cybersecurity Resource Center, *State of K-12 Cybersecurity 2020 Year in Review* 3-4 (2021), *available at* https://k12cybersecure.com/year-in-review/.

[119] CoSN, *State of EdTech Leadership in 2020* 16-17 (2020), *available at* https://www.cosn.org/focus-areas/leadership-vision/state-edtech-leadership.

[120] *What Is Least Privilege & Why Do You Need It?*, Beyond Trust (Nov. 17, 2016), https://www.beyondtrust.com/blog/entry/what-is-least-privilege.

[121] *See* Bill Siegel, Coveware, Inc., Prepared Written Testimony 8-9, Senate Committee on Homeland Security and Governmental Affairs (Dec. 2, 2020), *available at* https://www.hsgac.senate.gov/subcommittees/fso/hearings/rescheduled-state-and-local-cybersecurity-defending-our-communities-from-cyber-threats-amid-covid-19.

[122] See generally, Laird & Quay-de la Vallee, *Data Deletion*, *supra* note 20.

[123] IBM, *Security Services 2014 Cyber Security Intelligence Index* 3 (2014), *available at* http://www.corporate-leaders.com/sitescene/custom/userfiles/file/White_Papers/Cyber%20Security%20Intelligence%20Index.pdf.

[124] Hampton et al., *Broadband and Student Performance Gaps*, *supra* note 104, at 30.

[125] In its Order establishing the Emergency Connectivity Fund, the Federal Communications Commission clarified that "CIPA does not apply where schools or libraries have purchased advanced telecommunications and information services . . . to be used only in conjunction with student-, school staff- or patron-owned computers." *Establishing Emergency Connectivity Fund to Close the Homework Gap*, WC Docket No. 21-93, Report & Order, FCC 21-58 at 51-52, para. 108 (2021), *available at* https://www.fcc.gov/document/fcc-launch-717-billion-connectivity-fund-program-0.

[126] Hampton et al., *Broadband and Student Performance Gaps*, *supra* note 104, at 30-32.

[127] Cody Venzke, *Connecting Students with Digital Literacy Training*, Center for Democracy & Technology (Sept. 3, 2020), https://cdt.org/insights/connecting-students-with-digital-literacy-training/.

[128] *Avoiding Social Engineering and Phishing Attacks*, CISA (Oct. 22, 2009, rev'd Aug. 25, 2020), https://us-cert.cisa.gov/ncas/tips/ST04-014.

[129] *Digital Citizenship Curriculum*, Common Sense Education, https://www.commonsense.org/education/digital-citizenship/curriculum (last visited May 21, 2021).

[130] Hannah Quay-de la Vallee, *A Security Checklist for School-Provided Technology*, Center for Democracy & Technology (Jul. 27, 2020), https://cdt.org/insights/a-security-checklist-for-school-provided-technology/.