
YOUR HOME, THE NEW CLASSROOM: HOW PUBLIC-SCHOOL ZOOM
USE ENCROACHES INTO FAMILY PRIVACY

Caroline A. Foster*

I. Introduction

When COVID-19 struck the world in mid-March 2020, school closures in the United States prompted school officials to restructure learning to an online platform.¹ As a result of this transition to online learning, Zoom quickly rose to the forefront of platforms utilized by schools due to its video conferencing capabilities.² Zoom became a desirable platform for educators because it removed video chat time limits for K–12 schools in the United States and the platform has many

* J.D. Candidate, Suffolk University Law School, 2022.

¹ See Holly Peele, Maya Riser-Kositsky & Hyon-Young Kim, *Map: Coronavirus and School Closures in 2019-2020*, EDUC. WEEK (Mar. 6, 2020) [hereinafter *Map*], archived at <https://perma.cc/JM9R-HFYD> (noting that the coronavirus pandemic caused a near-total closure of schools in the spring of 2020). “Nearly every state either ordered or recommended that schools remain closed through the end of the 2019–20 school year.” *Id.* See also Cathy Li & Farah Lalani, *The COVID-19 pandemic has changed education forever. This is how*, WORLD ECON. F. (Apr. 29, 2020), archived at <https://perma.cc/P5JC-YQDG> (recognizing a rise of e-learning and teaching being done remotely and on digital platforms).

² See Alex Konrad, *Exclusive: Zoom CEO Eric Yuan Is Giving K-12 Schools His Videoconferencing Tools For Free*, FORBES (Mar. 13, 2020) [hereinafter Konrad, *Zoom CEO*], archived at <https://perma.cc/NLV8-LLUG> (noting that amid the pandemic, Zoom emerged as one of the resources that kept students learning). As of March 11, 2020, “343,000 people globally downloaded the Zoom app, 60,000 in the U.S. alone.” *Id.*

features that are useful for online learning.³ Nevertheless, the negative impact of Zoom use in schools quickly came to light in terms of its infringement on privacy rights of both students and families.⁴

Zoom insists that it takes the privacy rights of its customers very seriously, trying to accommodate for both expressed and potential privacy concerns.⁵ Further, the company released a privacy statement

³ See *id.* (describing how Zoom CEO Eric Yuan removed time limits from video chats for certain Zoom users, including K–12 schools affected by the virus in Japan, Italy, and the United States); Sophie Heller, *Zoom Features for Teachers*, OUTSCHOOL (Apr. 4, 2021), archived at <https://perma.cc/H7EW-QRLA> (listing features on Zoom that are helpful for teachers, such as text chat, screen sharing, annotation, and breakout rooms). Zoom also gives teachers the option to switch between speaker and gallery view, mute participants, remove a student if they are being disruptive, and disallow students from changing their onscreen name. Heller, *supra*.

⁴ See Valerie Strauss, *School districts, including New York City's, start banning Zoom because of online security issues*, THE WASH. POST (Apr. 4, 2020), archived at <https://perma.cc/ZM4S-NWPN> (mentioning how school districts around the country have begun to ban Zoom use for learning due to security concerns); Mark Lieberman, *Zoom Use Skyrockets During Coronavirus Pandemic, Prompting Wave of Problems for Schools*, EDUC. WEEK (Apr. 6, 2020), archived at <https://perma.cc/QQ9M-VCS8> (noting that privacy advocates and public officials are angry with Zoom's privacy policy). See also Robby Soave, *When Teachers Call the Cops on Parents Whose Kids Skip Their Zoom Classes*, REASON (Aug. 17, 2020), archived at <https://perma.cc/2G2X-5EQA> (recognizing that teachers in Massachusetts can contact authorities if a student does not come to Zoom classes to report parents for suspected child abuse); Aaron Feis, *Colorado school calls sheriff on boy, 12, who showed toy gun in virtual class*, N.Y. POST (Sept. 7, 2020), archived at <https://perma.cc/ES98-8BL4> (discussing how a 12-year-old boy was suspended for playing with a toy gun while in Zoom class); Hannah Sparks, *Mom can't stop laughing after accidentally flashing daughter's Zoom class*, N.Y. POST (May 27, 2020), archived at <https://perma.cc/5TUJ-AJRQ> (describing how a mother accidentally walked naked in the background of her child's Zoom class); Natalie O'Neill, *Florida mom shot dead in middle of her child's Zoom class*, N.Y. POST (Aug. 12, 2020), archived at <https://perma.cc/DM3E-3B4V> (noting that students witnessed a murder take place while in class on Zoom); Ailsa Chang, *To Report Abuse, Or Not? Zoom Classes Create Dilemma For Teachers*, NPR (Nov. 5, 2020), archived at <https://perma.cc/BYG2-VE32> (highlighting how a class of 7-year-olds saw one of their peers get sexually assaulted during virtual class); Paul Best, *Florida parents reportedly smoking weed, drinking during kids' remote classes*, FOX NEWS (Sept. 18, 2020), archived at <https://perma.cc/R2ZP-G8N9> (describing how parents have been seen drinking and smoking in the background of their child's Zoom classes).

⁵ See Letter from Zoom's Management Team to Client (Aug. 5, 2020) [hereinafter Letter], archived at <https://perma.cc/B7SH-LR84> (detailing privacy and security

for Zoom users in K–12 schools, revealing a higher standard of protection for this demographic.⁶ Despite the precautions the platform is taking to minimize privacy concerns, schools utilizing Zoom can force students to use certain features—such as turning on their video cameras—infringing on the privacy rights of those within the video frame.⁷ Not only are students attempting to adapt to a lack of social interaction and routine as a result of the switch to online learning, but they also have to cope with balancing privacy while following school protocols.⁸

K–12 schools should not use Zoom as an alternative method of learning during the COVID-19 pandemic—and future events that prompt school closures—due to the potential infringement on students’ privacy rights. While the Fourth Amendment of the United States Constitution (“Fourth Amendment”) provides that students have a lower expectation of privacy while in public schools, the ability for educators, as well as school officials and fellow students, to now see

measures Zoom is implementing). According to the letter, Zoom has “actively and quickly addressed specific security concerns as they were raised over the past few weeks. Zoom absolutely delivers a safe and secure virtual meeting environment when used with the appropriate safeguards to protect meetings.” *Id.*

⁶ See *Zoom for K-12/Primary and Secondary Schools Privacy Statement*, ZOOM (July 2020) [hereinafter *Zoom for K-12*], archived at <https://perma.cc/NHT6-KAAF> (describing the privacy protection of student users). Student users are not allowed to create K–12 accounts if they are under the age of 16, but they can join a Zoom meeting hosted by a K–12 Account User. *Id.* School Subscribers are also required to obtain parental consent in order to use the Services under their K–12 Accounts by Student Users. *Id.*

⁷ See Sydney Johnson, *On or off? California schools weigh webcam concerns during distance learning*, EDSOURCE (Aug. 26, 2020) [hereinafter Johnson, *On or off?*], archived at <https://perma.cc/L6DC-ZFGA> (describing how some districts in California require students to have their webcam on during class). See also Tabitha Moses, *5 reasons to let students keep their cameras off during Zoom classes*, THE CONVERSATION (Aug. 17, 2020), archived at <https://perma.cc/9KUR-8Y6J> (listing five reasons why students should be allowed to keep their webcams off in class, those being increased anxiety and stress, “Zoom fatigue,” competing obligations, right to privacy, and financial means and other kinds of access).

⁸ See Edward Roesch, *How The Shift To Remote Learning Affects Students Used To Face-To-Face Learning*, ELEARNING INDUS. (June 17, 2020), archived at <https://perma.cc/FJJ7-WRZG> (recognizing how the pandemic left students with an abrupt change in lifestyle due to the lack of social interaction and routine, among other things); Tom Armelino, *As schools go to distance learning, key strategies to prevent learning loss*, EDSOURCE (July 17, 2020), archived at <https://perma.cc/E4UX-FPX2> (outlining how the pandemic affected students’ social, emotional, and academic needs).

inside—and enter—the private homes of students and parents is very different than the Fourth Amendment’s intended scope. Particularly, schools forcing students to use their webcams while attending class is an infringement of students’ privacy rights due to the invasive nature of this feature. If schools allowed for optional webcam use, Zoom may prove appropriate in the public-school setting, but there are still other questionable privacy concerns. In the event that Zoom use in schools becomes a standard, the government must update the Family Educational Rights and Privacy Act (“FERPA”) and other educational based acts that address student privacy in order to account for the privacy infringements that are occurring as a result of virtual education due to COVID-19.

II. History

A. *The Fourth Amendment*

Citizens’ privacy rights stem from the Fourth Amendment.⁹ In order for an individual to assert their right to privacy under the Fourth Amendment, they must exhibit a subjective expectation of privacy that society recognizes as reasonable.¹⁰ Individuals have a subjectively

⁹ See U.S. CONST. amend. IV (defining the scope of an individual’s right to privacy). The Fourth Amendment reads as follows:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id. See also *Schmerber v. Cal.*, 384 U.S. 757, 767 (1966) (noting that the purpose of the Fourth Amendment is to “protect personal privacy and dignity against unwarranted intrusion by the State”); *Mapp v. Ohio*, 367 U.S. 643, 650 (1961) (describing that “security of one’s privacy against arbitrary intrusion by the police” is at the core of the Fourth Amendment). Further, “the Fourth Amendment’s right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth” Amendment, and the Fourth Amendment is “enforceable against them by the same sanction of exclusion as is used against the Federal Government.” *Mapp*, 367 U.S. at 655. See generally U.S. CONST. amend. XIV (extending the Fourth Amendment guarantee against unlawful searches and seizures to the states).

¹⁰ See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (recognizing that there is a two-prong requirement for privacy rights). First, a person

reasonable expectation of privacy when they take measures to ensure privacy in their location, whether that location is their own personal home or a public telephone booth with a door they can close.¹¹ However, citizens can waive their right to privacy if they act in a manner that exposes their private affairs to the world.¹² Even if an individual is within their private home, their right to privacy can be unintentionally waived if they expose their matters to the world, such as conducting their actions in front of an open window or talking loudly on the phone on their front porch.¹³

Typically, probable cause is needed in order for police to conduct a search or seizure that would otherwise invade one's right to privacy.¹⁴ Nevertheless, probable cause is not needed in every

must exhibit an actual (subjective) expectation of privacy, and second, that expectation of privacy must be one that society recognizes as reasonable. *Id.*

¹¹ *See id.* at 360 (holding that an “enclosed telephone booth is an area where, like a home . . . a person has a constitutionally protected reasonable expectation of privacy”). When an individual uses a telephone booth, the person “shuts the door behind him, and pays the toll that permits him to place a call,” entitling the individual to assume that his conversation is private. *Id.* at 361. “The point is not that the booth is ‘accessible to the public’ at other times, but that it is a temporarily private place whose momentary occupants’ expectations of freedom from intrusion are recognized as reasonable.” *Id.*

¹² *See id.* (noting that “a man’s home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited.”). Thus, there is an unreasonable expectation of privacy when one expects conversations in the open to be protected from being overheard. *Katz*, 389 U.S. at 361.

¹³ *See id.* at 351 (highlighting how “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”). On the other hand, “what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” *Id.*

¹⁴ *See* FED. R. CRIM. P. 41(d)(1) (asserting that a magistrate issues a warrant to seize a person or property if there is probable cause). *See also* Overview of the Fourth Amendment, 49 GEO. L. J. ANN. REV. CRIM. PROC. 3, 16 (2020) (noting that probable cause is required for most governmental intrusions on privacy interests covered by the Fourth Amendment). Probable cause to search has been defined by the Supreme Court as “a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.* at 16–17. Further, “probable cause exists when police have, at the moment of arrest, knowledge of facts and circumstances grounded in reasonably trustworthy information sufficient in itself to justify a belief by a prudent person that a suspect has committed or is committing an offense.” *Id.* at 17. *See also* *Illinois v. Gates*, 462 U.S. 213, 267 (1983) (holding that probable cause is determined using a totality of the circumstances approach).

situation, as there are exceptions to this requirement.¹⁵ One recognized exception arises in “special needs” cases.¹⁶ Under the aforementioned exception, there is no requirement for a warrant or probable cause in certain programmatic searches when these searches are performed in furtherance of a governmental “special need” as opposed to criminal investigation purposes.¹⁷ One commonly recognized group that is susceptible to searches under the special needs exception is public school students.¹⁸

1. The Reduced Scope of the Fourth Amendment with Students

The Supreme Court of the United States (“Supreme Court”) recognizes that students in the school environment or on school grounds have a lesser expectation of privacy than citizens who are not in school.¹⁹ Public school students are also susceptible to a higher degree of governmental intervention than private school students due

¹⁵ See Overview of the Fourth Amendment, *supra* note 14, at 4 (verifying that the Fourth Amendment does not require probable cause or a warrant, and there are developed exceptions to the warrant and probable cause requirement).

¹⁶ See Warrantless Searches and Seizures, 49 GEO. L. J. ANN. REV. CRIM. PROC. 51, 51 (2020) (noting that one valid exception to the Fourth Amendment probable cause and warrant requirement is when the “special needs of law enforcement make the probable cause and warrant requirements impracticable.”).

¹⁷ See *id.* at 165 (describing the special needs exception). There is a two-pronged test to evaluate if there is a special need. *Id.* at 165–66. First, the special need must be furthered “beyond the normal need for law enforcement,” and the government’s interest must be a “real, current, or vital problem that the proposed search effectively addresses.” *Id.* at 166–67. Second, the reasonableness of the search is evaluated by “balancing the nature of the intrusion on the privacy interest at stake against the government interest served by the search.” *Id.* at 167. Determining the permissibility of special needs searches are fact and case specific. *Id.* See also *Ashcroft v. al-Kidd*, 563 U.S. 731, 736 (2011) (listing instances where the special needs exception applies). Several situations where no warrant or probable cause is needed under the special needs exception are when there is a governmental need to deter drug use in public schools and ensure railroad employees are not under the influence of drugs or alcohol when working. *Id.*

¹⁸ See *Bd. of Educ. v. Earls*, 536 U.S. 822, 829 (2002) (recognizing that special needs exist in the public-school context); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (concluding that the special needs exception applies in public schools).

¹⁹ See *N.J. v. T. L. O.*, 469 U.S. 325, 348 (1985) (Powell, J., concurring) (recognizing a lesser expectation of privacy for students on school property).

to the school being governmentally operated.²⁰ Nonetheless, students do not “shed their constitutional rights . . . at the schoolhouse gate.”²¹ This diminished constitutional protection granted to students is mostly a result of school officials’ need to maintain discipline and order within the school.²² Courts balance the interests of both the students and the school officials by recognizing qualitative differences between the constitutional remedies for both students and adults.²³ Due to this

²⁰ See *The Federal Role in Education*, ED GOV (May 25, 2017), archived at <https://perma.cc/4YJT-6SB8> (laying out the government’s role in education). Education is a state and local responsibility, and the Department of Education is part of the Executive Branch. *Id.* See Ashley Rogers Berner, *The Case for Educational Pluralism in the U.S.*, MANHATTAN INST. (July 2019), archived at <https://perma.cc/975A-WQLH> (highlighting how “public education in the U.S. has been defined as schools that are funded, regulated, and exclusively delivered by government.”). See also *Pierce v. Soc’y of Sisters*, 268 U.S. 510, 534 (1925) (recognizing the public’s interest in the quality of private schools, allowing some government involvement). States have the responsibility to

reasonably . . . regulate all schools, . . . inspect, supervise and examine them, their teachers and pupils; to require that all children of proper age attend some school, that teachers shall be of good moral character and patriotic disposition, that certain studies plainly essential to good citizenship must be taught, and that nothing be taught which is manifestly inimical to the public welfare.

Id. See also *Runyon v. McCrary*, 427 U.S. 160, 178 (1976) (showing that the State can get involved when private schools have racially discriminatory admissions policies). “[W]hile parents have a constitutional right to send their children to private schools and a constitutional right to select private schools that offer specialized instruction, they have no constitutional right to provide their children with private school education unfettered by reasonable government regulation.” *Id.*

²¹ See *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503, 506 (1969) (observing that “[i]t can hardly be argued that either students or teachers shed their constitutional rights to freedom of speech or expression at the schoolhouse gate.”). See also *Acton*, 515 U.S. at 681 (O’Connor, J., dissenting) (confirming that students still have rights on school property). See also Julie A. Tappendorf, *Vernonia Sch. Dist. v. Acton: Now Children Must Shed Their Constitutional Rights at the Schoolhouse Gate*, 18 HAW. L. REV. 869, 891 (1996) (recognizing a retreat in protecting students’ First Amendment constitutional rights over the years).

²² See *T. L. O.*, 469 U.S. at 349 (Powell, J., concurring) (describing school officials’ need to discipline).

²³ See *id.* (describing the balance the Court seeks between students’ privacy rights and school officials’ need to discipline). In balancing these competing interests, Justice Powell identifies the student’s ability to return home at the end of the school day and the commonality of interests shared between teachers and their students. *Id.* at 349–50. On the other hand, Justice Powell identifies the State’s need to ensure

diminished right to privacy, schools are able to act in ways that further governmental interests without the need to obtain a warrant, even if those actions invade the privacy rights of students.²⁴ When a school official conducts a search of a student, the search will be “justified at its inception” when there are reasonable justifications for believing that the search will uncover evidence that the student has violated or is violating either a law or the rules of the school.²⁵ This standard is appropriate in the school setting because of its focus on reasonableness.²⁶ Teachers and school officials utilize their reason and common sense when searching a student instead of the harder probable cause standard, and the search invades a student’s privacy only to the extent necessary to uphold school order.²⁷ This standard adequately balances the privacy interests of students and the need for school officials to maintain order.²⁸

schools meet their responsibility of educating and training students, which can only be done through establishing discipline and maintaining order. *Id.* at 350.

²⁴ See *Acton*, 515 U.S. at 653 (recognizing that in the public-school context, the warrant requirement would interfere with disciplinary procedures needed by the schools, and the probable cause requirement would undermine the school officials’ need to maintain order). While searches can be based on individualized suspicion, there is no requirement that there be any suspicion. *Id.*

²⁵ See *T. L. O.*, 469 U.S. at 341–42 (clarifying what makes a search reasonable in a school setting). The search will be considered reasonable when the measures used are reasonably related to the objectives of the search and not overly intrusive, taking into account the age and sex of the student as well as the nature of the infraction. *Id.* at 342. See also Barry C. Feld, *T.L.O. and Redding’s Unanswered (Misanswered) Fourth Amendment Questions: Few Rights and Fewer Remedies*, 80 MISS. L. J. 847, 848–49 (2011) (recognizing that by upholding the search under an amorphous reasonableness standard, the Court in *T. L. O.* left little guidance for schools or courts when defining valid searches in schools).

²⁶ See *T. L. O.*, 469 U.S. at 341–42 (highlighting the main focus of the “justified at its inception” approach as focusing on the question of what is reasonable).

²⁷ See *id.* at 342–43 (detailing how the reasonableness standard works).

[T]he standard will spare teachers and school administrators the necessity of schooling themselves in the niceties of probable cause and permit them to regulate their conduct according to the dictates of reason and common sense. At the same time, the reasonableness standard should ensure that the interests of students will be invaded no more than is necessary to achieve the legitimate end of preserving order in the schools.

Id. at 343.

²⁸ See *id.* at 342–43 (recognizing the balancing of this test is to ensure that both the privacy rights of the students are protected while also allowing schools to keep

School officials have found there to be legitimate governmental interests in certain privacy invasions of students on school property, including, but not limited to, drug testing and ensuring the safety of students.²⁹ Courts have even found these rights to extend off school property in certain circumstances if there remains an interest for school officials to maintain order, such as school sponsored field trips.³⁰ However, there are limitations on the scope of what school

order). This test allows for school officials to avoid worrying about the complexities of determining if there is probable cause to search and instead use reason and common sense. *Id.* at 343. This intrusion by the school officials also takes into account the privacy right of the students and ensures that their privacy rights are invaded no broader than what is needed for preserving order at school. *Id.*

²⁹ See *Bd. of Educ. v. Earls*, 536 U.S. 822, 838 (2002) (concluding that drug testing students who are involved in extracurricular activities serves the school's interest in protecting the health of students); *Acton*, 515 U.S. at 664–65 (holding that the Student Athlete Drug Policy that requires all students who participate in interscholastic athletics to undergo random urinalysis drug testing is reasonable); *T. L. O.*, 469 U.S. at 347 (holding that it was reasonable for the principal to search a student's purse when he saw rolling papers next to the cigarette pack because there was reasonable suspicion to believe marijuana paraphernalia would be found); *Vassallo v. Lando*, 591 F. Supp. 2d 172, 197–98 (E.D.N.Y. 2008) (finding it reasonable for a school official to search a student's backpack and person in relation to a fire started in the bathroom); *Mac Ineirghe v. Bd. of Educ.*, No. 05-CV-4324, 2007 U.S. Dist. LEXIS 61841, at *29 (E.D.N.Y. 2007) (finding it was reasonable for the school after finding a student outside during school hours and with visible signs of possible drug use to take his vital signs, search his backpack and shoes, pat-down his pockets, and give him a saliva-based drug test).

³⁰ See *Webb v. McCullough*, 828 F.2d 1151, 1157 (6th Cir. 1987) (holding it was reasonable while on a school field trip for the principal to search the student's hotel room due to his dual authority under his role as school official and *loco parentis*). While the students were on a field trip in Hawaii, the Court held it was reasonable for the principal to search the student's room for alcohol, drugs, and any other items that violated the rules of the trip. *Id.* at 1152–53. The Court also noted that the principal's authority to search the room fell both under his authority as principal and under his authority of *loco parentis*. *Id.* at 1157. While the Court specified that the *loco parentis* doctrine does not apply when students are just going to school, it applied in this case because this was a school trip over 5,000 miles away from home and it required parental permission. *Id.* In application of the *loco parentis* doctrine, the Court considered the fact that there are many more ways for a student to be injured or ignore school rules during a non-curricular field trip than in school, therefore justifying granting increased authority to school officials. *Id.* Additionally, since there is a greater range of activities that take place during extracurricular activities than in school, school officials should have more authority to intervene. *Id.*

officials can search, showing that schools do not have endless authority over students and their belongings.³¹

2. Incorporating Technology into the Fourth Amendment

When drafting the Fourth Amendment, the Framers could not have foreseen the difficulties that would arise with the advancement and progression of technology.³² In particular, the development and advancement of police surveillance techniques creates issues for many courts when determining a search's reasonableness.³³ Historically, courts utilize the two-prong test from *Katz v. United States* when determining if there is a valid privacy interest.³⁴ Typically, there is no reasonable expectation of privacy when an individual knowingly exposes their private matter to the world or voluntarily gives private information to a third party, such as a bank or a telephone company.³⁵

³¹ See *In re William G.*, 40 Cal. 3d 550, 567 (1985) (holding that the search of the student's calculator was not reasonable because there were no facts to support reasonable suspicion). The assistant principal thought he had authority to search the calculator case because it had an "odd-looking bulge" and the student put it behind his back when the assistant principal approached. *Id.* at 555. The Court concluded that the search was illegal, and the evidence found from the search required suppression. *Id.* at 567.

³² See Russell L. Weaver, *THE FOURTH AMENDMENT, PRIVACY AND ADVANCING TECHNOLOGY*, 80 Miss. L. J. 1129, 1131 (2011) (recognizing that the Framers would not have known the effects that technology would have on the Fourth Amendment).

³³ See *id.* at 1132 (noting the new techniques that officers can utilize when conducting a search). Police can plant microphones to overhear conversations, use devices that pick up conversations through walls, use forward-looking infrared to surveil heat emanating from houses, use technology to detect speeding motorists, use global positioning systems ("GPS") to surveil the location of individuals and things, use devices to overhear phone conversations, use x-ray technology to look through walls and into homes using drive-by x-ray vans, and use devices to monitor key strokes and other computer uses through spyware technology. *Id.* at 1133–34.

³⁴ See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (describing the two-prong test).

³⁵ See James J. Tomkovicz, *TECHNOLOGY AND THE THRESHOLD OF THE FOURTH AMENDMENT: A TALE OF TWO FUTURES*, 72 Miss. L. J. 317, 346 (2002) (noting what society does not recognize as a reasonable expectation of privacy). See also *California v. Greenwood*, 486 U.S. 35, 41 (1988) (recognizing that "police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public.");

In applying the two-prong test to cases involving police officers using technological means to search and gather evidence, courts have found many instances where no invasion of privacy took place.³⁶ However, there are cases where the Supreme Court held that certain technological tools created an invasion of a legitimate expectation of privacy, revealing the tension when applying Fourth Amendment principals to advancing technology.³⁷ In determining

United States v. Miller, 425 U.S. 435, 443 (1976) (noting that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).

³⁶ See Florida v. Riley, 488 U.S. 445, 450–51 (1989) (holding that aerial surveillance of a partially covered greenhouse in a residential area from a helicopter does not violate one’s reasonable expectation of privacy); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that aerial surveillance using an aerial mapping camera to take images not visible to the naked eye did not violate a reasonable expectation of privacy that society recognizes); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that no legitimate expectation of privacy was violated when the police used aerial observation without a warrant from an altitude of 1,000 feet of a fenced-in backyard within the curtilage of a home to see if marijuana was being grown); United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding that examining and chemically testing a white powdery substance on a damaged package, concealed within eight layers of wrappings, did not violate any expectation of privacy because it was only saying whether or not it was contraband); United States v. Knotts, 460 U.S. 276, 285 (1983) (holding that instillation of a beeper, a radio transmitter that emits signals that can be picked up by a radio receiver, on a chloroform drum to see where it was traveling invaded no legitimate interests of privacy of the defendant); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the instillation and use of a pen register did not violate the defendant’s expectation of privacy because dialed phone numbers are turned over to third parties).

³⁷ See Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that accessing historical cell phone records that provide information on the user’s past movements violates one’s expectation of privacy); Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of a thermal imaging device from the outside street to detect heat within a private home violates one’s reasonable expectation of privacy); United States v. Karo, 468 U.S. 705, 716 (1984) (holding that installing a beeper on a can of ether that entered the private home of the defendant, a location not open to visual surveillance, violated the defendant’s expectation of privacy). *Karo* differs from *Knotts* because in the latter case, there was no Fourth Amendment violation of privacy because a beeper was placed inside a container of chloroform, and it did not reveal information that could not have been obtained through visual surveillance of the naked eye. *Karo*, 468 U.S. at 707. See also Tomkovicz, *supra* note 35, at 358 (recognizing that *Kyllo* is the first case that “takes a long overdue and significant first step by both explicitly and implicitly acknowledging the importance

what constitutes an invasion of privacy, courts have avoided creating a definitive rule, but they appear to convey that no invasion of privacy occurs when the technology is used only as a sensory enhancement tool.³⁸ On the other hand, there is an invasion of privacy when the technological tool invades and is used to interfere with the privacy of the home environment.³⁹

It is recognized that property interests, in addition to privacy interests, are protected under the Fourth Amendment; the Fourth Amendment prohibits the government from committing a trespass onto private property by using technological means.⁴⁰ In cases where this tension between the Fourth Amendment and the advancement of technology arises, the Supreme Court seems to draw a line of reasonableness once technology is used to allow the government to gain information relating to the interior of the private home, holding that there is a violation of privacy at that point.⁴¹ Further, the courts also seem to consider whether the technological device used to access

of understanding the tension that exists and arriving at sensible Fourth Amendment resolutions of the issues raised by technological enhancements of human capacities.”).

³⁸ See Weaver, *supra* note 32, at 1184 (recognizing that “if the police use technology merely as a form of sense enhancement, the use of that technology has generally been upheld” as not invading a privacy interest). Some of these sensory enhancement items include flashlights, electronic listening devices, plane flights, electronic beepers, and photographic equipment. *Id.* at 1220.

³⁹ See *id.* at 1184 (observing that technologies that are used to spy into the privacy of the home are often considered an invasion of privacy rights by the courts).

⁴⁰ See United States v. Jones, 565 U.S. 400, 404–05 (2012) (holding that by attaching a GPS tracking device to an individual’s vehicle and then using the GPS to track the vehicle’s movements on public streets, the government violated the defendant’s property rights).

⁴¹ See Tomkovicz, *supra* note 35, at 395 (noting that information received about the inside of a private dwelling from technological means is entitled to the privacy protection of the Fourth Amendment regardless of the quality of the information). In cases involving technology that receives information about the home’s interior, the Supreme Court does not distinguish between substantial and insubstantial information and between intimate and non-intimate information. *Id.* at 396. See also Payton v. N.Y., 445 U.S. 573, 590 (1980) (recognizing that at the core of the Fourth Amendment is the right of one to retreat into his home to be free from unreasonable governmental intrusion). “The Fourth Amendment has drawn a firm line at the entrance to the house.” *Id.* But see Katz v. United States, 389 U.S. 347, 351 (1967) (recognizing an exception where there is no Fourth Amendment protection in what a person knowingly exposes to the public, even if within the home).

the potentially private information is in “general public use.”⁴² If the technology is in “general public use,” there is a higher likelihood that police officers did not invade a privacy interest due to the device being accessible by non-law enforcement personnel.⁴³ Despite the advancement of technology and its broader use, science and technology should not have the power to decrease the privacy rights guaranteed by the Constitution.⁴⁴

B. Combining Education and Technology Under the Fourth Amendment

With the advancement of technology, schools have the ability to determine if they want to utilize these technological advancements on school grounds.⁴⁵ Over the years, schools have increased their use

⁴² See Tomkovicz, *supra* note 35, at 404–05 (noting that courts take into consideration whether “public use of the technology is ‘routine,’ is ‘sufficiently rare,’ or occurs ‘with sufficient regularity.’”).

⁴³ See *id.* at 405 (highlighting what constitutes a device being in general public use). “When tools that enhance ordinary human abilities to perceive and acquire information that would otherwise remain confidential are generally or routinely used by the public, official exploitations of those tools do not cross the Fourth Amendment threshold.” *Id.* See also *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (recognizing that using devices that are not in general public use to gain information of a home that would be unknowable without physical intrusion constitutes an invasion of privacy); *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (noting that private and commercial flights in public airways are routine, and thus it is unreasonable for the defendant to have an expectation of privacy in his marijuana plants).

⁴⁴ See Tomkovicz, *supra* note 35, at 437 (recognizing the need to uphold the privacy rights guaranteed in the Constitution despite technological advancements).

⁴⁵ See Mark Keierleber, *Inside the \$3 Billion School Security Industry: Companies Market Sophisticated Technology to ‘Harden’ Campuses, but Will It Make Us Safe?*, 74 MILLION (Aug. 9, 2018), archived at <https://perma.cc/NQ8T-NSJZ> (noting the increase in video surveillance in schools). Some schools utilize cameras that have analytics capabilities allowing authorities to be notified if the cameras detect unusual activity, such as someone going onto school grounds after school closure. *Id.* See Eli Zimmerman, *Company Offers Free Facial Recognition Software to Boost School Security*, ED TECH (Aug. 3, 2018), archived at <https://perma.cc/D9QH-C77T> (noting that a company offered to provide a facial recognition software for free to over 100,000 school districts); Austin Cushing, *What Should Schools Consider Regarding Metal Detectors and X-Ray Scanners as Security Measures?*, ANCHORTEX CORP. (Sept. 29, 2016), archived at <https://perma.cc/D85S-H8PA> (reporting that New York City has utilized handheld and walkthrough metal detectors and x-ray machines in 88 school buildings since a fatal shooting in a New York City school in 1992).

of technological tools.⁴⁶ Many schools are utilizing surveillance technology—such as video cameras—to monitor behavior, with some schools employing devices that use biometrics and artificial intelligence to obtain advanced results.⁴⁷ Nevertheless, these new technologies concern many schools because of their potential to invade the privacy rights of students.⁴⁸ Some states have taken measures to protect students' privacy rights in accordance with advancing technology, as seen by the passage of laws.⁴⁹ While some states like

⁴⁶ See Keierleber, *supra* note 45 (finding an increase in security cameras in schools over the years). In the 1999–2000 school year, only 19% of schools across the country used security cameras, and by the 2015–2016 school year, 81% of schools used security cameras. *Id.* The increase of surveillance in schools is due largely in part to prevent school shootings and create a safer school environment. *Id.* See Ankita Bhutani & Preeti Wadhvani, *Artificial Intelligence (AI) in Education Market Size Worth \$6bn by 2024*, GLOB. MKT. INSIGHTS (Aug. 12, 2019), archived at <https://perma.cc/FW9E-D6ER> (calculating that the use of Artificial Intelligence in the education market is “set to surpass USD 6 billion by 2024”).

⁴⁷ See Maya Weinstein, *School of Surveillance: The Students' Rights Implications of Artificial Intelligence as K–12 Public School Security*, 98 N.C. L. REV. 438, 441–42 (2020) (highlighting how many schools are responding to the need of enhanced school security with the implementation of emerging technologies). “While basic security cameras have been used as monitoring devices in schools for years, some schools are looking to more advanced technologies to gain a greater level of control over the campus environment.” *Id.* at 441. Some of the new technological advances that schools are implementing “include advanced cameras and body scanners, [which] use biometrics and artificial intelligence (“AI”) to recognize faces; detect weapons, gunshots, and other threats; and track individuals' locations in schools.” *Id.* at 441–42.

⁴⁸ See Zimmerman, *supra* note 45 (recognizing that while biometric data collection has its benefits, school officials have to balance that benefit with the privacy concerns involved with capturing this data of students); Weinstein, *supra* note 47, at 442 (recognizing a tension between protecting students from violence with these new technologies and invading a student's fundamental right to privacy); Amy Rhoades, *Big Tech Makes Big Data Out of Your Child: The FERPA Loophole EdTech Exploits to Monetize Student Data*, 9 AM. U. BUS. L. REV. 445, 447 (2020) (highlighting that “[w]ith the increase of technology use in schools, parents, students, and privacy advocates have growing concerns that current regulation is inadequate to meet the rapid advancing technology EdTech companies employ.”).

⁴⁹ See Andrew Ujifusa, *State Lawmakers Ramp Up Attention to Data Privacy*, EDUC. WEEK (Apr. 15, 2014), archived at <https://perma.cc/KUF5-BAVS> (noting that as access to educational data on students has grown, state lawmakers want to protect the students' privacy and security). In particular, in response to technological advances, “for the 2014 legislative sessions, 83 bills in 32 states have addressed student-data protection issues, according to the Data Quality Campaign, a Washington-based group that seeks to promote the use of educational data to inform

New York are creating state-level positions to work with education agencies and make recommendations on how to protect student data, other states like Florida are prohibiting the collection of student biometric information.⁵⁰ The states that are attempting to protect student data through legislation are doing so through a variety of different approaches, but all aim to regulate student data privacy and assure its protection.⁵¹

Students also have certain privacy rights under FERPA, preventing schools from sharing “personally identifiable information.”⁵² Personally identifiable information includes, but is not limited to: a student’s name; the name of the student’s parents or family members; the student’s address; a personal identifier; an indirect identifier; and information that is linkable to a student and

classroom and policy decisions.” *Id.* See also NEV. REV. STAT. § 388.272 (2014) (requiring that schools have privacy and security provisions when entering into contracts with data service providers); FLA. STAT. § 1002.222 (2014) (recognizing that agencies and institutions cannot “collect, obtain, or retain” biometric information of a student).

⁵⁰ See Ujifusa, *supra* note 49 (outlining laws states have made to protect student data). “As part of a budget deal approved by lawmakers, [New York] will create a new position of chief privacy officer to work with local education agencies and make recommendations about the best ways to protect student data.” *Id.* On the other hand, “[a] bill that passed the [Florida] Senate . . . would prohibit collection of students’ biometric data, such as fingerprints and retinal information.” *Id.* Similarly, Kansas tried to pass a bill that would prohibit the collection of biometric data. *Id.* Idaho also passed a law that “vests authority over student-data use with the state board of education, which has to file annual reports about what types of student data are being collected and any breaches in data security. It also requires districts to adopt policies governing student data.” *Id.*

⁵¹ See *id.* (describing the best bills as ones that “establish clear responsibilities and policies for data without necessarily eliminating certain types of data from being collected at all.”). In drafting these bills, “[s]tates need to balance the desire for data protection and security with the significant value such information can have on states’ longitudinal data systems as well as local school districts’ efforts to craft better instructional practices.” Ujifusa, *supra* note 49.

⁵² See Weinstein, *supra* note 47, at 466 (noting that FERPA is a federal law that protects certain privacy rights). See also Family Educational and Privacy Rights, 20 U.S.C.S. § 1232g (2013) (outlining the privacy rights of students); *Family Educational Rights and Privacy Act (FERPA)*, ED GOV (Dec. 15, 2020) [hereinafter *FERPA*], archived at <https://perma.cc/K46M-GF9M> (describing FERPA). Under FERPA, personally identifiable information is distinguished from directory information which can be disclosed without parental consent, and directory information includes, “a student’s name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.” *FERPA, supra.*

allows others to easily identify the student.⁵³ Congress enacted FERPA to maintain student and parental privacy rights over a student's educational records, and it attempts to govern the "collection, maintenance, and disclosure" of certain information related to the student's education.⁵⁴ In order for information to be considered a confidential student record under FERPA, the information must directly relate to the student and be maintained by the school.⁵⁵ However, two exceptions to FERPA—the "health and safety exception" and the "school officials exception"—allow school

⁵³ See 34 C.F.R. § 99.3 (2011) (outlining what constitutes personally identifiable information for FERPA purposes). Personal identifiers consist of a student's social security number, student number, or biometric record, and indirect identifiers refer to a student's date of birth, place of birth, and mother's maiden name. *Id.* See also Weinstein, *supra* note 47, at 468 (recognizing that the 2008 update to FERPA "clarified that a student's biometric record includes 'fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.'").

⁵⁴ See Sarah Pierce West, *They[ve] Got Eyes in the Sky: How the Family Educational Rights and Privacy Act Governs Body Camera Use in Public Schools*, 65 AM. U. L. REV. 1533, 1539 (2016) (observing that "one of the primary goals of FERPA was to 'protect such individuals' rights to privacy by limiting the transferability of their records without their consent."). FERPA aims to protect the privacy rights of students in their educational records, and it protects the rights of parents to inspect and review their child's records. *Id.* at 1540. An educational record may include, but is not limited to, "student discipline files, grades, standardized testing results, or other records in written, video, electronic form, or other forms of media," and they do not necessarily need to be academic in nature. *Id.* at 1542. The record can also include, "immunization records, photographs, or student employment information." *Id.* See also *Owasso Indep. Sch. Dist. No. I-011 v. Falvo*, 534 U.S. 426, 429 (2002) (defining an educational record as "'records, files, documents, and other materials' containing information directly related to a student, which 'are maintained by an educational agency or institution or by a person acting for such agency or institution.'").

⁵⁵ See Rhoades, *supra* note 48, at 449–50 (describing what is considered a private student record under FERPA). The Department of Education considers "factors such as the activity depicted, the intended uses by the educational institution, and whether the image contains [personally identifiable information] otherwise found in the student's record" when determining if it is protected. *Id.* The Department of Education does not consider "student images incidentally captured, as in the background of a photo" to be protected under FERPA. *Id.* The record also must be maintained by the school or an agent of the school to be considered an educational record. *Id.* In terms of online data, FERPA excludes information exchanged by an email or messaging application that is not maintained by the school, for example an email between a student and teacher that is not centrally located. *Id.* at 450–51. See also *Falvo*, 534 U.S. at 435 (observing that "FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar").

officials to intrude on student's protected rights in particular circumstances.⁵⁶ Under the "health and safety exception," schools can release protected student information if there is an "actual, impending, or imminent emergency"—such as a natural disaster, terrorist attack, or campus shooting—and the information released must be related to that emergency.⁵⁷ In terms of the "school officials exception," schools can disclose private student records to school officials without needing to obtain consent.⁵⁸

⁵⁶ See Weinstein, *supra* note 47, at 466 (recognizing two privacy exceptions under FERPA). The "health and safety exception" "gives schools 'greater flexibility and deference' to disclose educational records without consent to 'appropriate parties,' which could include law enforcement or emergency responders, among others." *Id.* at 469. The "school officials exception" allows "[e]ducational agencies and institutions [to] disclose [personally identifiable information] from education records without consent to school officials (including School Resource Officers), provided they meet the school's criteria for 'school officials' with 'legitimate educational interests.'" *Id.* at 470. See also FINAL REPORT OF THE FEDERAL COMMISSION ON SCHOOL SAFETY 129–33 (Dec. 18, 2018) [hereinafter FINAL REPORT], *archived at* <https://perma.cc/8HW5-GTVU> (highlighting how FERPA's "health and safety exception" works); SCHOOL RESOURCE OFFICERS, SCHOOL LAW ENFORCEMENT UNITS, AND THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) 10–11 (Feb. 2019) [hereinafter SCHOOL RESOURCE OFFICERS], *archived at* <https://perma.cc/HNV5-TUR2> (describing who constitutes a school official under the "school officials exception").

A "school official" may include . . . a teacher, school principal, president, chancellor, board member, trustee, registrar, counselor, admissions officer, attorney, accountant, human resources professional, information systems specialist, and support or clerical personnel. Contractors, consultants, volunteers, or other third parties to whom a school or district has outsourced certain functions may also be considered "school officials."

SCHOOL RESOURCE OFFICERS, *supra*.

⁵⁷ See Weinstein, *supra* note 47, at 469 (outlining when protected student information can be released under the "health and safety exception"). See also *When is it permissible to utilize FERPA's health or safety emergency exception for disclosures?*, ED GOV (Oct. 15, 2019), *archived at* <https://perma.cc/VRY2-BRZH> (recognizing that the exception relates to serious matters, such as a natural disaster, terrorist attack, school shooting, or outbreak of an epidemic disease); 34 C.F.R. § 99.36 (2021) (noting that the decision to release the information is based on a totality of the circumstances in relation to the health and safety of the students).

⁵⁸ See Weinstein, *supra* note 47, at 470 (recognizing how if a person meets the requirements of a "school official" with "legitimate educational interests," no consent is required to obtain a student's private educational records). This exception leaves a lot of discretion to the schools to define who qualifies as a "school official." *Id.* See also 34 C.F.R. § 99.31 (2021) (outlining who can qualify as a school official under the exception).

Further, students may not recognize the intrusiveness of some technologies utilized by schools, especially if they are of a younger age, leading students to forfeit their privacy rights without fully understanding the consequences.⁵⁹ Some of the facial recognition technology produced has a harder time identifying younger people, making it problematic if schools use this technology in the school setting.⁶⁰ Schools also already utilize technology as a way to monitor what students do beyond the walls of the classroom by observing what students do online, potentially invading their privacy rights even when students are not physically on school grounds.⁶¹

⁵⁹ See Weinstein, *supra* note 47, at 443 (noting that “[s]tudents may not understand the extent to which their personal information is being collected and shared”). Further, students might not realize that some facial detection machines are inherently biased, inaccurately reading the faces of women and people of color. *Id.* at 455. If these biased technologies are used to determine who is involved in an incident or who is allowed to enter the school, students of color will be at risk of being misidentified as individuals who committed conduct violations or are otherwise prohibited from entry. *Id.* at 457. See also Christina Couch, *Ghosts in the Machine*, PBS (Oct. 25, 2017), *archived at* <https://perma.cc/Z3U8-78DG> (outlining that “facial detection algorithms made in the U.S. are frequently trained and evaluated using data sets that contain far more photos of white faces, and they’re generally tested and quality controlled by teams of engineers who aren’t likely to have dark skin.”).

⁶⁰ See Weinstein, *supra* note 47, at 457 (recognizing that facial recognition technology has a higher rate of inaccuracy with younger faces). See also Couch, *supra* note 59 (recognizing that facial recognition algorithms are less accurate when identifying younger people).

⁶¹ See Weinstein, *supra* note 47, at 449 (noting that “some schools are already monitoring their students online, using Safety Management Platforms as threat assessment measures to scan school computers for indicators of violence by analyzing the words students type.”). See also Simone Stolzoff, *Schools are using AI to track what students write on their computers*, QUARTZ (Aug. 19, 2018), *archived at* <https://perma.cc/5DRS-K4PG> (recognizing that students using school computers will likely have what they do online tracked). This tracking on school computers can even extend to school-issued Chromebook laptops and tablets. *Id.* While some schools might just block inappropriate websites, others may employ software companies to gather potentially worrisome student behavior and report it to school officials. *Id.* See also Michael Goodyear, *The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of U.S. Data Privacy Law*, 10 HOUS. L. REV. 76, 85 (2020) (recognizing that in 2010, the Lower Merion School District in Pennsylvania provided laptops to students that were taking pictures of the students). The laptops had web cameras that could be activated if the laptops were stolen, but instead of being limited to that circumstance, the laptops took pictures of the users in the privacy of their homes. *Id.*

III. Premise

A. *Online Learning in the Midst of COVID-19*

1. Coronavirus Outbreak and Closure of the United States

With the continued spread of coronavirus cases worldwide and the increase of cases within the United States, the Trump Administration declared a public health emergency on February 3, 2020.⁶² By March 13, 2020, former President Donald Trump declared the coronavirus a national emergency and issued a travel ban on foreign travelers as cases continued to increase in an effort to mitigate the spread of the deadly disease.⁶³ As cases of the virus continued to rise despite governmental action, states began taking their own measures to slow the spread of the disease, with some going as far as issuing stay-at-home orders.⁶⁴ As a greater number of states began

⁶² See *A Timeline of COVID-19 Developments in 2020*, AJMC (July 3, 2020) [hereinafter *Timeline*], archived at <https://perma.cc/SY83-NGGM> (noting that the coronavirus was declared a public health emergency in the United States by early February). The United States' declaration that the virus was a public health emergency came three days after the World Health Organization ("WHO") declared a global health emergency as the cases rose to 9,800 worldwide and there were 200 deaths. *Id.* The first known case of the coronavirus in the United States was discovered in an individual in Washington on January 21, 2020. *Id.*

⁶³ See *id.* (recognizing that this declaration opened funding to limit the virus's spread). See also Proclamation No. 9994, 85 Fed. Reg. 15,337 (Mar. 13, 2020) (recognizing the coronavirus as a national emergency). Trump "[f]ound] and proclaim[ed] that the COVID-19 outbreak in the United States constitute[d] a national emergency, beginning March 1, 2020." *Id.*

⁶⁴ See *Timeline*, *supra* note 62 (noting that California was the first state to issue a stay-at-home order on March 19, 2020). California's stay-at-home order required all residents to stay home unless they needed to go to an essential job or shop for essential needs. *Id.* See also Sarah Mervosh, Denise Lu & Vanessa Swales, *See Which States and Cities Have Told Residents to Stay at Home*, THE N.Y. TIMES (Apr. 20, 2020), archived at <https://perma.cc/2BED-QUZR> (listing the states and if and when stay-at-home orders were implemented). While only nine states had statewide stay-at-home orders on March 23, 2020, by March 30, 2020, thirty states had statewide orders. *Id.* See also Dialynn Dwyer, *Charlie Baker urges travelers not to come to Mass. communities and to self-quarantine if they do*, BOSTON (Mar. 27, 2020), archived at <https://perma.cc/396H-WHBC> (noting that Massachusetts urged travelers who came into the state to quarantine for fourteen days). This recommendation was made in tandem with the recommendation that residents stay at home and the closure of nonessential businesses. *Id.*

issuing stay-at-home orders across the country, many K–12 schools were forced to close by early March to help prevent the spread of the virus.⁶⁵ As schools continued to close across the country, determining how students would learn without physically coming to school arose as a major issue.⁶⁶

2. Determining How Public Schools Could Operate During the Pandemic

Many school districts took action and moved learning to online platforms in order to continue school despite the ongoing pandemic.⁶⁷ Districts encountered the issue of determining how their schools would provide the necessary means for students to connect virtually, whether it be providing students with Chromebooks and internet access or students already having the necessary means to participate in virtual learning.⁶⁸ Several of the options available to school districts were

⁶⁵ See Lauren Camera, *Coronavirus Closes Schools for Half of All Kids In the U.S., Now What?*, US NEWS (Mar. 16, 2020), archived at <https://perma.cc/4Q7J-BKAJ> (observing that by March 16, 2020, thirty-three states had ordered the closure of all K–12 schools). These closures meant that over half of the 51 million students across the United States were forced to stay home. *Id.*

⁶⁶ See *id.* (noting that many school districts are switching learning to online, supplying students with devices, schedules, and directions for parents). However, with online learning, three major questions arose with the closure of schools:

How will students who count on school for breakfast and lunch continue receiving those meals? How will students keep up with their coursework at home, or will they at all? And how flexible will state and federal officials be when it comes to schools not meeting academic requirements as a result of the pandemic?

Id. School closures disrupted more than just learning for some students, for some students will now face issues concerning food insecurity, lack of internet access, and parents unable to remain home and help. *Id.*

⁶⁷ See Benjamin Herold, *The Scramble to Move America's Schools Online*, EDUC. WEEK (Mar. 27, 2020), archived at <https://perma.cc/XMW4-C65D> (recognizing that many schools were taking learning to online platforms to continue teaching from afar). According to a survey conducted on March 24–25, 60% of teachers were assigning and collecting work online and over 30% were using technology to teach live classes. *Id.* See also *Coronavirus and Learning: What's Happening in Each State*, EDUC. WEEK (Apr. 3, 2020), archived at <https://perma.cc/EE7U-ND7Y> (outlining what each state is doing in terms of school during the pandemic).

⁶⁸ See Sydney Johnson, *Thousands of California students to get free Wi-Fi and Chromebooks for distance learning*, EDSOURCE (Apr. 1, 2020) [hereinafter Johnson, *free Wi-Fi*], archived at <https://perma.cc/36XJ-UDRS> (noting that Google donated

providing printable worksheets, giving lessons through public television, using free online learning sites, using online platforms where students could communicate and upload their work, and live learning through video conferencing.⁶⁹ Most districts and states sent out “response plans” to inform schools, families, and students as to how the schools would operate with the continued spread of the virus.⁷⁰ Video conferencing platforms were a popular option for

4,000 Chromebooks and free Wi-Fi to 100,000 households in California); *4.4 million households with children don't have consistent access to computers for online learning during the pandemic*, USA FACTS (Sept. 28, 2020) [hereinafter *4.4 million households*], archived at <https://perma.cc/8CWC-4YNP> (recalling data from a survey that expresses how many households have internet access and computers).

According to the survey;

Of the 52 million households with children present, 74% always had access to a computer for educational purposes in September and 16% had access most of the time. An additional 8%, or 4.4 million households, had a computer available sometimes, rarely, or never. In households where a computer was always available, 60% received devices from the child's school or school district.

The numbers are similar for internet access.

4.4 million households, supra. At the time of the survey, 4.4 million households with students did not have consistent access to a computer, and 3.7 million did not have access to the internet. *Id.*

⁶⁹ See Herold, *supra* note 67 (recognizing that while some schools were limited to only photocopying worksheets, others were having teachers give lessons on public television through school partnerships with television networks). Other school districts utilized free online learning sites such as Khan Academy, and others used learning platforms such as Canvas and Google Classroom where students could upload their work. *Id.* Further, some utilized platforms that allowed for live learning. *Id.*

⁷⁰ See Letter from Kevin R. Fitzgerald to Caesar Rodney Families (Apr. 1, 2020) [hereinafter Letter from Kevin], archived at <https://perma.cc/P6EP-GJVU> (describing what the Caesar Rodney School District in Delaware was doing in terms of teaching). The superintendent notified families that in addition to using Clever and Schoology, teachers will use Zoom to stay in touch with students. *Id.* The superintendent also informed parents that they can opt their child out of Zoom, and he notified families to get in touch with the student's teacher if they do not have access to a computer or the internet. *Id.* See also *Continuity of Learning and COVID-19 Response Plan (“Plan”) Application Template*, MICHIGAN GOV (Feb. 5, 2021) [hereinafter *Continuity of Learning*], archived at <https://perma.cc/LAUW-AXRE> (requiring school districts in Michigan to submit a plan for how they were going to teach during the pandemic). Michigan noted how districts were at different states of readiness as to how they intended to operate, but it was “expected that schools will provide instruction at a distance using a variety of methods that meet local needs, including printed materials, phone contact, email, virtual learning, or a

school districts due to the live learning feature and having the ability to see students face-to-face.⁷¹ Despite the several video conferencing platforms available to school districts, many schools chose to utilize Zoom as their method of teaching.⁷²

combination to meet student needs.” *Id.* See also GEORGIA DEPARTMENT OF EDUCATION, STATE BOARD OF EDUCATION WAIVERS FOR LOCAL EDUCATION AGENCIES: RESPONDING TO THE COVID-19 PANDEMIC 6 (Mar. 31, 2020), archived at <https://perma.cc/L6GW-GKSL> (listing three approaches the Georgia Department of Education recognized as possible strategies for learning during the pandemic but does not mandate). The three approaches were limited instruction, supplemental instruction, and wholesale instruction. *Id.* With any approach utilized by a district, “[t]he Georgia Department of Education (GaDOE) strongly encourages districts to be sensitive about the realities students and staff are dealing with, including but not limited to challenges accessing devices/internet connectivity, caring for siblings/loved ones, and other roles/responsibilities during the COVID-19 pandemic.” *Id.* See also NEW HAMPSHIRE DEPARTMENT OF EDUCATION, NEW HAMPSHIRE GRADES K-12 BACK-TO-SCHOOL GUIDANCE ii (Mar. 2021), archived at <https://perma.cc/E6Q7-G4UH> (acknowledging that the guide is not a “one-size-fits-all” document). “[I]t recognizes the varied local contexts of each school district and acknowledges that many districts may develop their own operational guidelines utilizing this document as their base of minimum requirements.” *Id.*

⁷¹ See Larry Dignan, *Online learning gets its moment due to COVID-19 pandemic: Here’s how education will change*, ZD NET (Mar. 22, 2020), archived at <https://perma.cc/3W63-SFYL> (noting that video conferencing platforms, like Zoom and WebEx, are being used frequently). See also Rani Molla, *Microsoft, Google, and Zoom are trying to keep up with demand for their now free work-from-home software*, VOX (Mar. 11, 2020), archived at <https://perma.cc/9GAX-6Z26> (noting that companies like Zoom, Microsoft, and Google started offering their software for free and took measures to assist with the increased demand of their product); Lucy Handley, *‘I don’t know exactly what the secret is’: Zoom’s marketing chief on the company’s rise through the pandemic*, CNBC (July 24, 2020), archived at <https://perma.cc/JR88-XH6V> (recognizing how video conferencing platforms saw an increase in users during the pandemic). Specifically, Zoom had approximately 173 million monthly active users as of May 27, 2020, up from 14 million on March 4, 2020, and Microsoft Teams reached 75 million users on April 29, 2020, up from 44 million as of mid-March 2020. Handley, *supra*.

⁷² See Konrad, *Zoom CEO, supra* note 2 (recognizing that Zoom is one of the leading tools being used to educate children during the pandemic). Since Zoom’s April 2020 IPO, the company’s stock has outpaced its biggest rivals, including Microsoft Corporation and Cisco Systems, Inc., showing the platform’s success. *Id.* See also Goodyear, *supra* note 61 (noting the increase in use of Zoom at the start of the pandemic). “Since the start of March 2020, its stock price has risen 101% and its app has soared in popularity in the App Store to number eleven.” *Id.* See also Carmen Reinicke, *Zoom Video has seen its stock spike more than 100% since January as coronavirus pushes millions to work from home (ZM)*, BUS. INSIDER

B. Zoom as a Video Conferencing Platform

Eric Yuan created Zoom in 2013 after leaving Cisco Systems, Inc. (“Cisco”) due to his dissatisfaction with Cisco’s WebEx video conferencing platform and seeking to create a better product.⁷³ Yuan desired to create a video conferencing product that worked equally well “in a board room in Manhattan or from a kitchen table in China.”⁷⁴ Zoom, an attractive product for users because of certain differences it has from its competitors, does not need different versions for Macs and PCs, shields from bugs that browsers may introduce, and can work on low or spotty internet connection.⁷⁵ Zoom also has features that make the platform attractive to teachers, such as the ability to record audio

(Mar. 23, 2020), *archived at* <https://perma.cc/RE2A-X7G5> (recognizing that Zoom is having record outperformance in the stock market due to the pandemic). “As of March 18, Zoom cloud meetings ranked first in iPhone daily downloads among business apps in the US, and first by overall apps and games.” *Id.*

⁷³ See David Pierce, *Zoom conquered video chat — now it has even bigger plans*, PROTOCOL (Mar. 16, 2020), *archived at* <https://perma.cc/23TP-6WCL> (noting how Yuan quit his job at Cisco to pursue creating Zoom); Alex Konrad, *Zoom, Zoom, Zoom! The Exclusive Inside Story Of The New Billionaire Behind Tech’s Hottest IPO*, FORBES (Apr. 19, 2019) [hereinafter Konrad, *Zoom!*], *archived at* <https://perma.cc/5G3F-MJB9> (recognizing that Yuan was an “engineer-turned-founder who once ran engineering for Cisco’s WebEx video-conferencing business”). Yuan left Cisco because he thought WebEx had problems with its service to customers. Konrad, *Zoom!*, *supra*.

The service simply wasn’t very good. Each time users logged on to a Webex conference, the company’s systems would have to identify which version of the product (iPhone, Android, PC or Mac) to run, which slowed things down. Too many people on the line would strain the connection, leading to choppy audio and video. And the service lacked modern features like screen-sharing for mobile.

Id. When Cisco would not let Yuan rebuild the product, he left the company. *Id.*

⁷⁴ See *id.* (noting how Yuan wanted to create a product that was accessible to everyone).

⁷⁵ See *id.* (recognizing some of the perks Zoom has in comparison to its competitors).

Its lightweight Web client could figure out almost instantly what kind of device you were using, meaning Zoom didn’t need different versions for Mac or PC. It also provided a software layer that shielded any bugs that might be introduced when a browser like Chrome, Firefox or Safari pushed an update. Zoom could operate even at 40% data loss, so it would still work on a spotty or slow internet connection.

Id.

and video and save chat transcripts.⁷⁶ Teachers appreciate that Zoom is taking initiative to create features that are useful for an online classroom setting, including the capability to create a virtual seating chart, annotate the screen, put students into breakout rooms, and enable a whiteboard function.⁷⁷

C. *Privacy and Security Concerns Related to Zoom Use in Schools*

Due to Zoom's main use as a video conferencing platform, there are privacy and security concerns that Zoom attempts to mitigate.⁷⁸ Further, public schools have heightened concerns with the platform because of the need to protect students, and Zoom has addressed the need to take the privacy of students into account with

⁷⁶ See Lieberman, *supra* note 4 (recognizing some of Zoom's features that teachers found useful in the school setting). Not only was the 40-minute conferencing feature removed from Zoom when the pandemic started for all K–12 schools, but teachers also liked having the ability to video and audio record the classes and save chat transcripts. *Id.* Zoom users can also display two screens at the same time which teachers found to be helpful. *Id.*

⁷⁷ See Tain Barzso, *4 New Zoom Features Educators Can Use to Enhance Virtual Teaching & Learning*, ZOOM (Sept. 21, 2020), archived at <https://perma.cc/5DJZ-FEWY> (describing four new features Zoom created to help teachers in the virtual setting). The features include creating a virtual seating chart, the ability to pin multiple people on the screen, "spotlighting" participants to help when students are presenting, and a feature that helps with unmuting students. *Id.* See Erin Wilkey Oh, *How are teachers using Zoom? Is it safe for students? Learn more about this popular distance learning tool.*, COMMON SENSE (Apr. 27, 2020), archived at <https://perma.cc/L3B8-8XHB> (detailing what tools teachers can use to interact with students). Some of the useful features include a whiteboard function where students can write on the screen and breakout rooms where students are put into smaller groups within the class to discuss and then the teacher can bring the entire class back together. *Id.* See Howard Bowen, *Using Zoom for School: What are the Pros & Cons?*, VCG (Aug. 28, 2020), archived at <https://perma.cc/XU49-J3SR> (highlighting positive features of Zoom). When presenting, teachers or students can annotate their screen. *Id.*

⁷⁸ See *Zoom Privacy Statement*, ZOOM (Aug. 2020), archived at <https://perma.cc/8HRW-UHEM> (outlining Zoom's privacy and security measures). The statement explains Zoom's practices when it processes your "'personal data,' which is information that relates to an identified or identifiable individual. To 'process' or 'processing' means any use of personal data including, transferring, collecting, recording, storing, using, analyzing, combining, disclosing or deleting it." *Id.*

certain features.⁷⁹ According to Zoom’s K–12/Primary and Secondary Schools Privacy Statement, the platform uses technical and organizational measures to protect information from unauthorized access, use, and disclosure.⁸⁰ Zoom also has a FERPA Guide which details how the platform complies with FERPA requirements in an attempt to protect the security and privacy of student users.⁸¹ Despite Zoom’s attempt to implement privacy and security measures, some schools across the country started to ditch Zoom for other video conferencing platforms due to privacy related concerns.⁸² One main

⁷⁹ See *id.* (recognizing that schools have additional privacy concerns and Zoom provides further privacy and security statements for K–12 users); *Zoom for K–12, supra* note 6 (explaining how Zoom handles personal information of student users); Anya Kamenetz, *Schools Ditch Zoom Amid Concerns Over Online Learning Security*, NPR (Apr. 6, 2020), *archived at* <https://perma.cc/5PZK-UL7D> (noting that Zoom updated a set of security tips for educators and updated the settings for its education-based users giving more control to teachers). In a statement to NPR, Zoom said, “Zoom is committed to providing educators with the tools and resources they need on a safe and secure platform, and we are in continued dialogue with various school districts about how Zoom can be of service during this time.” Kamenetz, *supra*.

⁸⁰ See *Zoom for K–12, supra* note 6 (detailing the security measures Zoom takes for K–12 students). According to the Statement, “Customer Content is encrypted in transit between any devices running a Zoom client and at rest when in permanent storage in the Zoom Cloud,” and to avoid uninvited participants accessing Zoom meetings, Zoom “enabl[ed] meeting passcodes and virtual waiting rooms by default for K-12 Accounts and configur[ed] default screen share settings to limit in-meeting content sharing.” *Id.* See also Letter, *supra* note 5 (including a data sheet regarding Zoom’s new and old security features that help to keep data safe).

⁸¹ See *FERPA Guide, ZOOM* (Oct. 2020), *archived at* <https://perma.cc/AE3E-DJ3W> (highlighting how Zoom complies with FERPA). According to the Guide, “[v]ideo recordings/streams, chat logs, transcripts, and other information collected or maintained by a School Subscriber while using Zoom’s services may be considered education records under certain circumstances.” *Id.* With several exceptions, parental consent is needed to disclose personally identifiable information within a student’s education records, and because Zoom is considered a “school official” for the purposes of FERPA, Zoom “may receive [personally identifiable information] through its contractual agreements with School Subscribers because Zoom is performing a service that furthers a ‘legitimate educational interest.’” *Id.* Zoom also takes measures to protect personally identifiable information from unauthorized access, use, and disclosure. *Id.*

⁸² See Kamenetz, *supra* note 79 (noting that schools in New York City, Washington, D.C., and Las Vegas discontinued their use of Zoom during the pandemic due to “security, privacy, harassment and other concerns.”). Instead of using Zoom, these schools switched to alternative video conferencing platforms like Microsoft Teams,

concern was “Zoom-bombing” which is when uninvited users get access to a Zoom meeting and enter the meeting, sometimes showing racist or pornographic imagery to students.⁸³ Despite the problems associated with the platform, Zoom is still in high use across the country, showing its vast popularity with educators.⁸⁴

Google Hangouts, and WebEx. *Id.* See Lieberman, *supra* note 4 (recognizing that some school districts discouraged teachers from using Zoom or banned the use of the platform). In Fairfax County in Virginia, school officials made teachers who were using Zoom stop and use a different platform due to privacy concerns. *Id.* In addition, public schools in a district in Nevada “‘made the decision to disable access to Zoom out of an abundance of caution’ in response to hacking incidents in virtual classrooms.” *Id.* See Mike Kennedy, *Some districts say no to Zoom over security concerns*, AM. SCH. & U. (Apr. 6, 2020), archived at <https://perma.cc/ABM8-95MM> (recognizing that school districts have banned the use of Zoom use for online learning due to security concerns). One district in Nevada said it would “disable access to Zoom out of an abundance of caution due to instances of hacking that created unsafe environments for teachers and students,” and a school in Utah said it would reevaluate the use of Zoom in their schools after a Zoom-bomber displayed pornography to an online class. *Id.*

⁸³ See Kamenetz, *supra* note 79 (describing what “Zoom-bombing” is). Schools are switching away from Zoom due to Zoom-bombing which is when non-members join an existing meeting. *Id.* Some of these Zoom-bombing incidents have people showing racist and pornographic imagery to the students. *Id.* See also Jeffrey Solochek, *Schools using Zoom should be careful, security expert warns*, TAMPA BAY TIMES (Apr. 1, 2020), archived at <https://perma.cc/E6DN-AAGN> (noting that Zoom-bombing “has surfaced to describe the hijacking of these virtual meetings by participants and, occasionally, outsiders with ill intent.”). Beyond the Zoom-bombing concerns are concerns about people getting access to a Zoom code they are not supposed to have and scammers sending out fake “phishing” links with the goal of luring unsuspecting children into possibly compromising situations. *Id.* Zoom is being targeted with all these concerns while other video conferencing platforms are not because Zoom “is openly accessible through an app and website with a free signup regardless of email or service provider. Other programs, such as Microsoft Teams, require additional layers such as having an Outlook account that many people don’t have.” *Id.*

⁸⁴ See Lieberman, *supra* note 4 (noting that many educators still use Zoom as a platform to teach remotely during the pandemic despite noted privacy concerns). Zoom has features that are attractive to teachers that the other platforms do not have, such as saving chat transcripts and audio and video recordings for later accessibility. *Id.* See also Mitch Tarica, *Zoom Selected by Los Angeles Unified School District*, ZOOM (July 2, 2020), archived at <https://perma.cc/E5U3-R6FY> (highlighting how Zoom and the Los Angeles Unified School District entered into an agreement with each other). The agreement “will provide unlimited access to virtual classrooms for nearly 30,000 educators and more than 600,000 students in Los Angeles Unified schools.” *Id.* According to the Chief Academic Officer for the District, “Zoom has

The concerns that several schools are addressing when deciding to discontinue the use of Zoom seem to ignore the true privacy concern: that schools are infringing on the student's privacy rights by allowing teachers to enter the private homes of students through the video camera feature.⁸⁵ At the beginning of the pandemic following the switch to remote learning via Zoom, issues arose quickly, surrounding the notion that teachers were allowed to “enter” the homes of their students through the video feature and contact authorities if they thought there was an issue.⁸⁶ While some parents

already been a platform of choice for thousands of teachers due to an intuitive user interface and reliable performance.” *Id.*

⁸⁵ See Tyler Sonnemaker, *As Zoom classes take over during the pandemic, edtech companies provide a lifeline, but only for schools and parents willing to surrender their students' privacy*, BUS. INSIDER (Oct. 13, 2020), archived at <https://perma.cc/DWE8-U6MR> (recognizing that “privacy advocates and education experts worry the increased reliance on edtech tools has forced parents to choose between keeping their kids' schooling on track and protecting their civil liberties”); Lieberman, *supra* note 4 (recognizing that students, as well as parents, need to be mindful as to what is happening in the backgrounds of the video); Sarah Schwartz, *As Teachers Livestream Classes, Privacy Issues Arise*, EDUC. WEEK (Aug. 20, 2020), archived at <https://perma.cc/N23Q-N9AB> (noting that students and teachers can see details about a student's “family life, what their house looks like, or how many other people are living there” through Zoom's video feature). A policy counsel at Privacy Rights Clearinghouse said, “If students are required to have their camera on, that's going to force some students to reveal personal information that they might not feel comfortable sharing.” Schwartz, *supra*. See Joshua Dunn, *What Teachers Spy in Homes over Zoom Winds up in Court*, EDUC. NEXT (Mar. 9, 2021), archived at <https://perma.cc/NXP4-7BSP> (acknowledging that “the remote teaching environment during the pandemic has raised the question of what counts as ‘the classroom.’”). See also Jenna Amatulli, *Zoom Can Track Who's Not Paying Attention In Your Video Call. Here's How.*, HUFF POST (Mar. 25, 2020), archived at <https://perma.cc/5BHE-937K> (noting that meeting hosts can even see who is paying attention on Zoom through its “attention tracking” feature “that identifies whether participants have clicked away from the active Zoom window for more than 30 seconds.”).

⁸⁶ See Soave, *supra* note 4 (calling attention to the fact that teachers in some districts can contact authorities when a student does not come to Zoom classes). In Massachusetts, the Department of Children and Families (“DCF”) “has the power to remove children from their homes and place them in foster care if agents suspect that kids are being mistreated, abused, or neglected—and DCF considers distance-learning no-shows to be possible abuse cases.” *Id.* DCF further notes several instances where teachers should contact authorities, some being that a student appears tired or hungry during a Zoom class. *Id.* See Massachusetts Department of Children and Families: A Tip Sheet for Educators (June 1, 2020), archived at

laugh about the matter—as when a mom accidentally walked behind her child’s camera with no clothes on—people should question the intrusive nature of the platform being used by educators as a way, in some instances, to suspend students.⁸⁷

One instance where a school used the video feature beyond its intended purpose occurred when a school in Colorado suspended a 12-year-old student for five days because he played with a toy gun while in his virtual class.⁸⁸ This 12-year-old student was not the only student suspended for playing with a toy gun in class, as many other states suspended students for this behavior as well.⁸⁹ Teachers are also punishing students for displaying political signs in their online learning backgrounds, showing that some teachers are infringing on students’ freedom of expression.⁹⁰ In addition, in Massachusetts,

<https://perma.cc/ZJR5-9VQK> (listing instances when a teacher should contact authorities). *See also* Feis, *supra* note 4 (recognizing that school officials called the sheriff on a 12-year-old boy who was playing with a toy gun while in virtual class). This student was later suspended for playing with that toy gun. *Id.* The boy’s father “agreed that school officials have to understand that the virtual classes necessitated by the COVID-19 pandemic have brought teachers into students’ homes, where expectations must be different from classrooms.” *Id.*

⁸⁷ *See* Sparks, *supra* note 4 (noting how a mother accidentally walked naked through the background of her child’s Zoom class).

⁸⁸ *See* Feis, *supra* note 4 (noting that the boy was suspended from his online schooling and sheriffs were sent to his house after a teacher notified the school principal that the student was playing with a “gun” while in her virtual class).

⁸⁹ *See* Kristie Cattafi, *Edgewater school called police after sixth-grader had Nerf gun during Zoom class*, NORTH JERSEY (Sept. 11, 2020), *archived at* <https://perma.cc/RVF5-H5FH> (detailing how a sixth-grader in New Jersey was suspended for playing with a toy gun during his virtual class); Gisela Crespo, *4th grader suspended for having a BB gun in his bedroom during virtual learning*, CNN (Oct. 4, 2020), *archived at* <https://perma.cc/E5G9-EHFL> (noting that a nine-year-old boy was suspended for having a BB gun in the background of his video during his virtual class); Lori Jane Gliha, *Jefferson County 11-year-old suspended for handling an Airsoft gun during online school*, KDVR (Sept. 3, 2020), *archived at* <https://perma.cc/LPR2-KZR9> (describing how a sixth grade student was suspended for playing with his Airsoft gun during a Zoom class); Dunn, *supra* note 85 (recollecting how a 12-year-old middle school student was suspended in Illinois when he stood up in a remote-learning class and unintentionally revealed a pellet gun behind his bed).

⁹⁰ *See* Dunn, *supra* note 85 (detailing instances where students were punished for displaying Trump banners in their online learning video frame). A high school chemistry teacher in New Jersey kicked out a student who refused to take down a Trump banner from his bedroom wall. *Id.* An English teacher at the same school also asked the student to take down the banner because it might cause a disruption.

teachers even have the authority to get the Department of Children and Families (“DCF”) involved based on students’ Zoom behavior, going beyond a suspension and questioning the parents’ parenting ability.⁹¹ There is also an instance at a university involving a hard of hearing student being berated by her professor over Zoom for not answering a question posed to her—an instance that could very easily happen at the K–12 level as well—showing how students are facing privacy issues that would not occur in a normal classroom setting.⁹² Furthermore, students are experiencing a new form of cyberbullying as other students are able to enter students’ homes over Zoom and bully students based on the aesthetics of the home/bedroom.⁹³ Schools often

Id. It was later acknowledged that the student had not violated any school rules by having the banner in his background. *Id.* Similarly, a chemistry teacher in California claimed he would remove a student from the digital classroom if the student did not take down a Trump banner. *Id.* The student handbook for the district in California says that the district “respects students’ rights to express ideas and opinions, take stands on issues, and support causes, even when such speech is controversial or unpopular,” making the teacher’s actions unacceptable. *Id.*

⁹¹ See Soave, *supra* note 4 (recalling instances where teachers have contacted DCF based on a student’s Zoom behavior). One parent recollected how “she received a call from [DCF]. The school had accused Quiles of neglect, she was told, because the 7-year-old missed class and homework assignments.” *Id.* Another parent was contacted by DCF because someone at the school “accused the mom of ‘general neglect’ based on ‘behaviors observed or disclosed during remote learning.’ The agency spent weeks investigating the matter, interrogating the mother and her son on everything from ‘the contents of her refrigerator to her son’s sleeping location.’” *Id.* A third parent “faced frequent threats from teachers that DCF would intervene if the children didn’t improve their virtual attendance.” *Id.*

⁹² See Yaron Steinbuch, *College professor put on leave after berating hearing-impaired student on Zoom*, N.Y. POST (Feb. 24, 2021), archived at <https://perma.cc/2FK3-XGPR> (depicting a professor yelling at a hard-of-hearing student for not answering his questions). The student could not hear her professor well, and she was not able to respond right away to his questions because her translator took a few seconds to translate what was said before she could hear it in her hearing aid. *Id.*

⁹³ See Brittany Wong, *How Remote Learning Has Changed The Nature Of School Bullying*, HUFFPOST (Sept. 18, 2020), archived at <https://perma.cc/WC57-UJXM> (observing that bullying is still happening over Zoom). While there are less opportunities to bully in person due to school closures, students can find different ways to cyberbully. *Id.* Some of Zoom’s features—video recording and teacher supervision of the chat function—make it easier for bullies to be supervised which could be viewed as lowering the chance of bullying online. *Id.* See also Courtney Fischer, *Cyberbullying migrating to Zoom during virtual learning*, ABC (Oct. 22, 2020), archived at <https://perma.cc/YUD9-JWC2> (observing that bullying has been

require their students to have their video camera on, forcing students to expose their private space to not only the teacher, but also to their peers.⁹⁴

As a result of students now attending class from the privacy of their homes, schools need to balance their leniency with the rules and maintaining order, especially when it comes to suspending and giving students detention.⁹⁵ Further, the intrusive nature of virtual learning extends beyond just impacting the students, as parents and siblings also need to be mindful as to what they do behind the screen of their child's or sibling's remote learning class.⁹⁶ Although seeing something occur

seen over Zoom during virtual class). Through virtual learning, students can now see into other students' homes, and "[f]or teens who have spent years creating and perfecting an online image that's different from real life, one Zoom view of their room or their house can destroy everything." *Id.*

⁹⁴ See *id.* (observing how students utilize the chat feature of Zoom to criticize other students' rooms while Zoom class is occurring).

⁹⁵ See Joe Heim & Valerie Strauss, *School discipline enters new realm with online learning*, THE WASH. POST (Sept. 15, 2020), archived at <https://perma.cc/ZAM4-55RH> (recognizing that school rules need to be applied to online school). Some schools have extended their normal behavior guidelines to the new virtual setting with several modifications, and students are realizing that school rules do not just disappear even though they are at home. *Id.* One effective way teachers maintain order is by controlling the microphone of students. *Id.* However,

online discipline extends well beyond limiting noisy outbursts during class time. Teachers are also finding themselves having to monitor issues from attendance and appearance to whether the dozens of children or teenagers on the screen in front of them are engaged, sitting still, keeping their cameras on, answering questions, not eating or drinking, not petting their dogs and not bickering with siblings.

Id. Teachers have admitted that it is a lot harder understanding what students need and the problems that are occurring over a virtual platform as opposed to when they were in a classroom. *Id.* See also SHAWN PAGE & DR. ANGELA HARGRAVE, VIRTUAL STUDENT CONDUCT EXPECTATIONS 3 (Feb. 2, 2021), archived at <https://perma.cc/D8NB-XT9X> (outlining Shelby County Schools' student conduct expectations for virtual school).

⁹⁶ See Sonnemaker, *supra* note 85 (recognizing the difficulty that comes with calling out a student's parent's behavior over Zoom). One science education associate professor noted, "Sometimes, if you stop instruction to respond to it in the moment, it can make the situation worse. So calling out a parent who's drinking a beer is really calling out the student, which isn't fair to the student who's not engaging in the behavior." *Id.* She further added that "while teachers should intervene if they're concerned about a child's safety, 'it's not the teacher's responsibility, though, to manage the parent's behavior.'" *Id.* See O'Neill, *supra* note 4 (noting that students

over the screen is not as impactful as seeing it in person—making it so students are less likely to be affected by what they see in the background of another student’s video frame—it is still important to consider the possible ramifications of this privacy invasion.⁹⁷ While there is legislation, like FERPA and the Children’s Online Privacy Protection Act (“COPPA”) that aim to protect children’s privacy, these acts are not doing enough to protect the rights of students in this remote learning era.⁹⁸

in a Zoom class witnessed the murder of a student’s mother). The teacher was able to mute the video, so the other students did not have to hear the altercation, and the student’s video then went black after being struck by a projectile. *Id.* See also Best, *supra* note 4 (describing how parents have been seen by others in Zoom classes drinking and smoking in the background). A Florida elementary school teacher said some parents were walking around unclothed while drinking and smoking during remote learning classes and said that parents “need to realize that there is a window into their homes during remote learning.” *Id.*

⁹⁷ See Chandra Johnson, *Face time vs. screen time: The technological impact on communication*, DESERET NEWS (Aug. 29, 2014) [hereinafter Johnson, *Face time vs. screen time*], archived at <https://perma.cc/SZ8J-ZH5A> (recognizing that less emotion is attached to witnessing something through a screen than in real life).

Think of it as the difference between looking at a picture of cool, green grass and actually walking barefoot in it. The problem is that the more people and children interact with a person or the real world through a screen rather than in real life, the less emotion is attached to the exchange.

Id. See also Philip M. Boffey, *Do Violent Video Games Lead to Violence?*, DANA FOUND. (Nov. 1, 2019), archived at <https://perma.cc/DKL5-WFKL> (observing that there is no evidence that playing violent video games leads to mass murders or killings). At most, there is a small effect, with Justice Antonin Scalia noting in an opinion, “[t]hey show at best some correlation between exposure to violent entertainment and minuscule real-world effects, such as children feeling more aggressive or making louder noises in the few minutes after playing a violent game than after playing a nonviolent game.” *Id.*

⁹⁸ See *Is the Invasion of Student Privacy the Price for Remote Learning?*, STARTPAGE (May 11, 2020) [hereinafter *Invasion of Student Privacy*], archived at <https://perma.cc/DD23-6D6C> (identifying two acts that are directed at protecting children’s privacy). COPPA “protects the privacy of children under the age of 13 by requiring parental consent to use websites that collect data.” *Id.* FERPA “protects the privacy of educational records.” *Id.* See also *Complying With COPPA: Frequently Asked Questions*, FED. TRADE COMM’N (July 20, 2020), archived at <https://perma.cc/J3MH-SJEZ> (describing COPPA). COPPA was enacted in 1998, and “[t]he primary goal of COPPA is to place parents in control over what information is collected from their young children online. The Rule was designed to protect children under age 13, while accounting for the dynamic nature of the Internet.” *Id.* See also FERPA, *supra* note 52 (describing FERPA); Kaleigh C.

IV. Analysis

A. Zoom Creates Different Privacy Concerns for Schools

Public schools are exploring a new frontier by moving learning online due to the pandemic, facing privacy concerns that have not been dealt with in the past.⁹⁹ When the pandemic started, schools were initially concerned with keeping students connected and still learning.¹⁰⁰ This initial concern minimized focus on protecting students' privacy rights, which created large-scale future issues.¹⁰¹ While students do have a lesser expectation of privacy while they are in a school environment and on school grounds, learning from an online platform within the comfort of their home is vastly different than physically attending school, participating in school sponsored field trips, or using school-supplied technology for educational purposes.¹⁰² Outside of an online platform, there is a need for schools to maintain order and control conduct that occurs, leading to a lesser

Fitzpatrick, *Student Data at Risk: A Multi-Tiered Approach for Massachusetts to Mitigate Privacy Risks While Utilizing Innovative Education Technology in Schools*, 16 J. HIGH TECH. L. 294, 305–06 (2016) (highlighting how there are no legal remedies when a school violates FERPA). At most, a school could lose federal funding if it violates FERPA. Fitzpatrick, *supra*, at 306.

⁹⁹ See Sonnemaker, *supra* note 85 (noting that the “rapid shift to virtual learning this spring has blurred the line between students’ homes and schools, immediately sparking privacy scandals”). School being online has brought “new and unexpected side effects” to learning that educators have not dealt with in the past. *Id.*

¹⁰⁰ See *id.* (claiming that Cheri Kiesecker, the co-chair of the Parent Coalition for Student Privacy, recalled, “Unless school districts really had privacy on their radar ahead of time, it was: ‘How do we keep students connected?’ And, ‘We’ll worry about the privacy issues later’”).

¹⁰¹ See *id.* (observing how schools never dealt with drawing a boundary between school and the home). An associate professor of learning technology noted, “We’ve gone from the separation between home and school to a complete breakdown of the boundaries between the two without really training teachers or parents and guardians or students for what that means for their own privacy and learning.” *Id.* Teachers, students, and parents are faced with learning how to use online teaching technologies effectively, safely, and legally. *Id.*

¹⁰² See *N.J. v. T. L. O.*, 469 U.S. 325, 348 (1985) (Powell, J., concurring) (recognizing that there are special characteristics of schools that make it unnecessary to give students the same constitutional protections given to adults and children not in a school setting).

expectation of privacy for the students.¹⁰³ When students are physically at school, parents trust that educators and supervisors will maintain order to ensure the safety of their children, as well as when students attend school sponsored field trips.¹⁰⁴ Similarly, if schools take the initiative to supply the students with school issued laptops or Chromebooks, parents expect that the schools take adequate measures to ensure safe use of the device.¹⁰⁵

Teachers still have to consider potential safety concerns that could arise in this remote era in connection to how they maintain order and control while teaching from an online platform.¹⁰⁶ Educators are faced with different safety concerns because students cannot physically harm other students or be a danger to the health and safety of others when there is solely interaction through a video camera.¹⁰⁷

¹⁰³ See *id.* at 348–49 (noting that the Court has recognized and affirmed the need for school officials and states to control conduct and maintain order within schools). In order to be able to educate and train students, schools have to establish means to maintain order and discipline. *Id.* at 350. There is also an obligation for schools to protect children—as well as teachers—from the conduct of other students, leading to a lesser protection of privacy rights than what is required under the Constitution. *Id.* See also Feld, *supra* note 25, at 847 (recognizing “[i]n addition to their educational mission, school officials have to maintain order, provide a safe environment in which to learn, and control guns, drugs, and violence on campus and nearby.”).

¹⁰⁴ See *id.* at 924 (noting that schools have a responsibility to “maintain discipline, health, and safety.”). See also *Webb v. McCullough*, 828 F.2d 1151, 1157 (6th Cir. 1987) (recognizing that on school field trips, students are left in the care and safety of school officials, and there are more ways for a student to be injured or to take advantage of school rules).

¹⁰⁵ See Stolzoff, *supra* note 61 (noting that school-issued tablets or Chromebooks must have technological guardrails installed on them to keep students safe). Under the Children’s Internet Protection Act, any U.S. school that receives federal funding must have an internet safety policy which extends to school-issued technological devices. *Id.* While some schools block student access to certain websites, others install software on the devices that will notify school officials if there is potentially harmful communication taking place on the device. *Id.*

¹⁰⁶ See *T. L. O.*, 469 U.S. at 353 (Powell, J., concurring) (recognizing the interplay between order and safety because “[t]he special need for an immediate response to behavior that threatens either the safety of schoolchildren and teachers or the educational process itself justifies the Court in excepting school searches from the warrant and probable-cause requirement.”).

¹⁰⁷ See, e.g., Feis, *supra* note 4 (noting that when a boy was seen on screen in his virtual class with a toy gun, school officials made a statement saying, “[s]afety will always be number one for our students and staff. We follow board policies and safety protocols consistently, whether we are in-person or distance learning,” yet a toy gun

While students can still bully others despite the switch to remote learning, there is an added element of supervision with online learning because teachers are able to save and record chats, showing that it may occur to a lesser extent.¹⁰⁸ The methods applied by educators for maintaining order online should reflect the novel situation of students learning from within their private homes.¹⁰⁹

Teachers telling students what they can and cannot do from within the privacy of their home is overstepping a boundary.¹¹⁰

seen on camera has no safety concerns). *But see, e.g., Webb*, 828 F.2d at 1157 (recognizing that on school field trips, the *loco parentis* doctrine applies). In this case, the principal was acting both as a school representative and in his *loco parentis* capacity when he searched the plaintiff's room for drugs and alcohol. *Id.* It is reasonable for the principal to act in this additional capacity on the field trip because "there may be a need for a greater range of intervention by an administrator than is the case when a student is only active within the relatively orderly confines of a school," and "there are many more ways for a student to be injured or to transgress school rules or laws during a non-curricular field trip than during relatively orderly school hours." *Id. But see, e.g., Vassallo v. Lando*, 591 F. Supp. 2d 172, 198 (E.D.N.Y. 2008) (recognizing that school officials have a "strong interest in protecting the safety and welfare of its students, including preventing fires in the school and preventing drug possession or use in the school.").

¹⁰⁸ See Wong, *supra* note 93 (observing that bullies may have less of an opportunity to bully in remote classes). According to one associate professor of learning technology, "bullies are not only deprived of those in-person opportunities to pick on other students, they're being supervised most of the time." *Id.* Not only are students rarely alone with other students unless they are placed in breakout rooms over Zoom, but their parents/guardians are also around to keep a better eye on their children. *Id.* Teachers also often record the Zoom classes and can supervise what is said in the chat function, adding another element of supervision. *Id.*

¹⁰⁹ See Heim & Strauss, *supra* note 95 (describing how schools are changing rules to accommodate for online learning). While some schools are extending "their normal behavior guidelines to the virtual classroom with a few modifications that factor in the home setting," other schools "have created a raft of new rules and regulations for their online learners." *Id.* See also PAGE & HARGRAVE, *supra* note 95, at 9 (listing out student expectations that are related to the virtual setting). See also Dunn, *supra* note 85 (observing that instead of "suspending students or kicking them out of class, teachers and school officials would do well to use these events as teachable moments by not overreacting").

¹¹⁰ See Heim & Strauss, *supra* note 95 (noting that teachers still need to have rules when using Zoom to maintain order). "Students are finding out that the comforts of home don't extend to the virtual classroom—even if the virtual classroom happens to be in their home." *Id.* One school even requires students to have their designated schoolwork area clear of anything that does not relate to the class. *Id.* See also PAGE & HARGRAVE, *supra* note 95, at 9 (listing what is expected from one school in this virtual learning period). According to the expectations, student work areas must be

Learning from within an individual's own home is vastly different than physically going to school to learn—or attending a school sponsored field trip—where there is a higher need to control student's behavior to maintain an orderly environment.¹¹¹ While there still remains the potential to influence other students over a virtual platform, as when a student sees another student—or parent—engaging in questionable behavior, teachers should be cognizant when telling students what they can and cannot do from within the confines of their own home, taking into account the student's privacy interest and the impact on other students witnessing the behavior.¹¹² There is less pressure for students to act in a similarly disruptive manner when they view their peer's actions over a screen rather than in person, showing how online teaching should naturally be more orderly than physically attending school.¹¹³ In addition, there is a large number of students who use their own technological devices to attend virtual classes—as opposed to Chromebooks offered by the school—making it so the government should prevent school officials from dictating and controlling what those students do on their personally owned devices.¹¹⁴ Students have

free of foreign objects, recording device must be positioned so teachers can observe both the working space and student, eating and drinking are not allowed, students should work in areas that are isolated from other individuals and pets, and additional electronic devices should not be kept or used in the area. *Id.*

¹¹¹ See *T. L. O.*, 469 U.S. at 339 (recognizing that teachers have a substantial interest in maintaining discipline in the classroom and on school grounds). This need is heightened by the rise of drug use and violent crimes that take place in schools. *Id.* Beyond simply educating students, schools have the “obligation to protect pupils from mistreatment by other children, and also to protect teachers themselves from violence by the few students whose conduct in recent years has prompted national concern.” *Id.* at 350 (Powell, J., concurring).

¹¹² See Johnson, *Face time vs. screen time*, *supra* note 97 (observing that less emotion is attached to a person/situation when the exchange takes place through a screen rather than in person). See also O'Neill, *supra* note 4 (noting that a student was in an online class with other students when her mother was murdered in the background); Best, *supra* note 4 (calling attention to how parents can be seen smoking and drinking in the background of remote learning classes in Florida). A teacher at Boca Raton Elementary in Florida also called attention to how parents can be seen in towels, underclothes, and bras, and how parents need to realize other students in the online class can see them in that state of dress. Best, *supra* note 4.

¹¹³ See Boffey, *supra* note 97 (recognizing no persuasive link between playing violent video games and engaging in violent behavior).

¹¹⁴ See Johnson, *free Wi-Fi*, *supra* note 68 (noting that Google supplied students in California with Chromebooks and Wi-Fi). San Francisco Unified supplied around 5,200 Chromebooks to students since the close of schools due to the pandemic, and

a right to privacy in their personal property, even while they are on school grounds, showing that teachers should respect a student's rights to use their personal property as they please, as long as the student is not disrupting the learning environment or violating school rules.¹¹⁵

B. Access to Personal Information from within the Home from Zoom Use

The amount of information obtained about the inside of a student's home while using Zoom to teach exceeds what is allowed under the Fourth Amendment.¹¹⁶ Not only does this invasion of privacy affect the students attending class virtually, but it also affects parents who are forced to have rules and regulations inside their own

Los Angeles Unified "authorized an emergency investment of \$100 million" to give laptops to students who do not have one. *Id.* Los Angeles Unified also entered a partnership with Verizon to offer internet access to students. *Id.* See also 4.4 million households, *supra* note 68 (recognizing that 74% of households with children always have access to a computer for educational purposes, and 73% of households with children always have access to internet for online learning). "In households where a computer was always available, 60% received devices from the child's school or school district." *Id.*

¹¹⁵ See *T. L. O.*, 469 U.S. at 339 (identifying a student's privacy interest in their personal property). "[S]choolchildren may find it necessary to carry with them a variety of legitimate, noncontraband items, and there is no reason to conclude that they have necessarily waived all rights to privacy in such items merely by bringing them onto school grounds." *Id.* Not only do students need to bring supplies needed for their studies, but they also might need keys, money, hygiene products, and things needed for extracurricular activities. *Id.*

¹¹⁶ See Sonnemaker, *supra* note 85 (recognizing that teachers were not given advice or direction on how to talk to students about setting up their virtual learning area at home "to ensure they aren't accidentally sharing private information" that could lead to bullying or reporting to the school or law enforcement). Kiesecker, the co-chair of the Parent Coalition for Student Privacy, questioned the actions of the school officials who dealt with the boy in Colorado who was playing with a toy gun in class saying, "Is that actually a Fourth Amendment violation of warrantless search and seizure because you didn't invite them in your home, yet your kid is getting suspended or police are being called because of something that was seen on Zoom." *Id.* Kiesecker also added, "Parents and students are upset enough that they're seeking attorneys and actually saying: 'You know what? You are violating my civil rights by requiring me to have my camera on and have the background of my home.'" *Id.*

home due to their student's virtual education.¹¹⁷ The government seems to draw the line at the private residence, recognizing that there is an invasion of privacy when technology interferes with one's home environment.¹¹⁸ Regardless of the information received, when the government uses technology to gain information about a private home, there is often an encroachment on privacy rights.¹¹⁹ Since most teachers record Zoom classes, public schools—and therefore the government—have recorded videos of what is taking place within those students' homes.¹²⁰ When determining if there is an invasion of one's right to privacy, courts do consider whether the technological device used to gain information is in "general public use."¹²¹ In

¹¹⁷ See *id.* (noting that "calling out a parent who's drinking a beer is really calling out the student, which isn't fair to the student who's not engaging in the behavior"). It is also not the teacher's responsibility to call attention to a parent's behavior unless that behavior could potentially be interfering with a student's safety. *Id.* See Dunn, *supra* note 85 (recognizing that families can find it intrusive for schools to treat their personal homes as extensions of the physical school). Schools are failing to take into consideration when disciplining students the challenging circumstances both families and children are facing with remote learning. *Id.*

¹¹⁸ See *Payton v. N.Y.*, 445 U.S. 573, 590 (1980) (claiming that at the core of the Fourth Amendment is the right for man to retreat into the safety of his home and be free from governmental intrusion); Weaver, *supra* note 32, at 1220 (recognizing that the Court is protective of the home environment and is likely to reject the use of technology to spy on individuals who are within their home).

¹¹⁹ See Tomkovicz, *supra* note 35, at 395 (recognizing that the "nature or amount of confidential information that can be revealed by a technological tool is irrelevant" if information comes from within the home). All information, regardless of its qualitative and quantitative nature is protected by the Fourth Amendment if the information came from within the home from using a technological device. *Id.* at 396. "If a technological tool is capable of revealing concealed details and is exploited in ways that enable the perception of those otherwise inaccessible details, the substantiality or intimacy of the matters perceived should not affect the determination of whether the Fourth Amendment threshold has been crossed." *Id.* at 397. See also *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding that using thermal imaging to detect heat from within a private home constitutes an unreasonable search).

¹²⁰ See Lieberman, *supra* note 4 (noting that teachers like using Zoom because they can record videos of the meeting); Wong, *supra* note 93 (observing that some teachers record their live online classes).

¹²¹ See Tomkovicz, *supra* note 35, at 405 (calling attention to what constitutes "general public use"). "When tools that enhance ordinary human abilities to perceive and acquire information that would otherwise remain confidential are generally or routinely used by the public, official exploitations of those tools do not cross the Fourth Amendment threshold." *Id.* However, the Supreme Court has not yet

addition, there usually is no reasonable expectation of privacy when an individual knowingly exposes their private matter to the world, even if the individual is within the confines of their private home.¹²²

Schools are using Zoom and other virtual platforms precisely for the product to be used within the students' home during the pandemic; thus, the government has entered the homes of students in order for learning to continue.¹²³ The government has already used Zoom information in police investigations regarding potentially criminal behavior, such as students playing with "guns" in class.¹²⁴ By using Zoom information under these circumstances, the government is showing that it is not afraid to use this information to its advantage in criminal investigations, even when students are merely playing with toys.¹²⁵ Zoom is also a technological device in "general public use,"

addressed the extent of public use necessary to invoke the "general public use" doctrine, leaving some room for ambiguity. *Id.* at 412. Once a technological device is known to be in high use across many users, it can be assumed that individuals who choose to use the device and potentially expose details about their private life no longer have a legitimate privacy interest. *Id.* at 413. Nevertheless, since the "general public use" doctrine hinges on acceptance by the general public of the potentially invasive technological device, society as a whole can express disapproval of the device in order to protect their privacy interests. *Id.* at 414.

¹²² See *id.* at 346 (recognizing that "[s]ociety is not prepared to recognize the reasonableness of an expectation of privacy if an individual has knowingly exposed the putatively private matter to the public or has voluntarily conveyed the supposedly secret facts to a third party who has agreed to convey those facts to the authorities.").

¹²³ See Herold, *supra* note 67 (noting that when the pandemic started, educators had to figure out how to teach students from afar). Due to the pandemic, "many of the nation's children are currently attending school in their beds and on their sofas and at their kitchen tables, alongside siblings and pets, with laptops and tablets and textbooks." *Id.*

¹²⁴ See Feis, *supra* note 4 (detailing how deputies were sent to the student's home to clarify that the gun he was playing with while in online class was a toy gun); Crespo, *supra* note 89 (noting that after a boy was seen playing with a toy gun while in his Zoom class, the teacher locked the student out of the class and police reported to his home); Gliha, *supra* note 89 (recalling that a police officer was sent to an 11-year-old's house after a teacher was reviewing a recording of online class and saw the boy playing with a toy gun). See also Soave, *supra* note 4 (recognizing that schools can contact DCF and have police go to homes if they think a student is being neglected through Zoom observance).

¹²⁵ See Crespo, *supra* note 89 (depicting the Louisiana Attorney General's disbelief in the situation). "I am alarmed by what appears to not only be multiple violations of both the State and Federal Constitutions, but also blatant government overreach by the school system," the Attorney General commented. *Id.* "For anyone to conclude that a student's home is now school property because of connectivity

with many people using it across the world either for school, meetings, work, or staying in touch with others.¹²⁶ However, students and parents have expressed their disapproval towards educators who use the device to invade the privacy rights of the students.¹²⁷ Using this virtual platform is also not so much a student choice, but rather a requirement imposed by the schools, creating doubt as to if the “general public use” doctrine can be applied to Zoom use in school settings.¹²⁸

Teachers often require students to use the video camera feature during virtual class, forcing the students to expose not only their private affairs, but also what is in the background of their computer cameras.¹²⁹ It is questionable whether students are “voluntarily”

through video conferencing is absurd . . . It is ludicrous for this All-American kid to be punished for taking responsible actions just as it is for his parents to be accused of neglect,” he added. *Id.*

¹²⁶ See Konrad, *Zoom CEO*, *supra* note 2 (naming Zoom as a leading tool to keep businesses running and students learning during the pandemic); Pierce, *supra* note 73 (recalling in early March, Zoom “reported 61% more business customers than the year prior” with “[m]ore than 10 million people join[ing] a Zoom meeting every day.”).

¹²⁷ See Sonnemaker, *supra* note 85 (noting that some parents and students are seeking legal action due to their privacy rights being infringed upon due to virtual learning).

¹²⁸ See Schwartz, *supra* note 85 (calling attention to how requiring students to utilize the camera feature forces them to reveal personal information that they might not feel comfortable sharing); see also Tomkovicz, *supra* note 35, at 414–15 (recognizing that society controls whether a technological device is in “general public use” based on approval or disapproval).

If the values jeopardized by widespread public use of a device that puts privacy at risk were sufficiently important, one might expect some indication of societal disapproval. If regular public use of a device to access our secrets breeds no evident resentment and provokes no restrictive reaction, one might logically infer a general sentiment that the harm done to privacy is tolerable.

Tomkovicz, *supra* note 35, at 414–15.

¹²⁹ See Johnson, *On or off?*, *supra* note 7 (noting that some school districts require students to keep their video feature on during virtual class). In California, “[w]hether a district wants to set rules around camera use is a local decision, and the state does not have any official guidance on whether cameras should be on or off during class.” *Id.* One student at a high school in San Jose said his teachers give him the option to turn on his camera, and he appreciates the decision because his “room is [his] private space. [He doesn’t] like having [his] camera on and people being able to look at it and judge [his] posters or how messy or clean it is . . . Being able to have [his] camera turned off gives an added sense of privacy.” *Id.* Some schools that require the camera feature to be on provided students with “backdrop[s]” of school mascots or logos, but backgrounds are not compatible with all technological devices. *Id.* Some

exposing what is within the background of the camera since they are often forced to turn it on and may not fully understand that what is within sight is being broadcasted to the whole class.¹³⁰ While teachers could take measures to remedy this such as asking students to check their workspaces before turning on their video cameras, it is unfair for educators to put the onus on the students, and even the parents, to comply with this suggestion.¹³¹ This is unacceptable when many students are sharing spaces with family members whose actions they are unable to control.¹³²

C. FERPA Considerations

FERPA is a federal law aimed at protecting the privacy of students, yet it does not take into account privacy concerns that are occurring due to virtual learning.¹³³ Critics of FERPA have pressured the U.S. Department of Education (“DOE”) to clarify FERPA’s scope and application in the recent years, and they have even requested that the DOE update FERPA to meet the privacy and security needs of

districts also allow students and families to sign an “opt-out” form if they wish to keep their camera off during virtual classes. *Id.* See also Lieberman, *supra* note 4 (recognizing that “[p]arents who consent to their students participating in class on video need to be mindful that other students and the teacher will be able to see what’s in the background”).

¹³⁰ See Johnson, *On or off?*, *supra* note 7 (recognizing that some students are forced to turn on their camera when using virtual platforms). See also Tomkovicz, *supra* note 35, at 346 (noting that there is no protection of the Fourth Amendment if one voluntarily exposes or shares their private affairs to others).

¹³¹ See PAGE & HARGRAVE, *supra* note 95, at 9 (highlighting how one school requires parents to take the extra measure to contact the student’s teacher if the student does not have an isolated working area). According to the Expectations, “When possible, students are encouraged to work in areas that are isolated from other individuals and pets. If circumstances exist that do not allow complete seclusion, the parent will need to share this information separately with the instructor. Instructors will only require what the parent can reasonably provide.” *Id.*

¹³² See Crespo, *supra* note 89 (noting that the student’s sibling, who shared a room with him, accidentally kicked his BB gun that was on the ground which prompted the student to pick it up); Soave, *supra* note 4 (commenting on how both DCF and the police department were contacted when a child’s six-year-old brother ran naked in front of the screen).

¹³³ See Weinstein, *supra* note 47, at 466 (describing FERPA as a federal law that “protects the privacy of student education records’ and ‘gives parents certain rights with respect to [those] records.’”). FERPA governs disciplinary records and grades, and it can include pictures and videos of the student as part of the record. *Id.*

advancing technology.¹³⁴ Further, the “health and safety exception,” as well as the “school officials exception,” to FERPA do not have clear standards that are readily applicable and understandable, making it even harder to apply FERPA to these unprecedented times.¹³⁵ In terms of the “health and safety exception,” there are many misconceptions in the education and law enforcement communities as to when student information can be shared, highlighting a need for the legislature to clarify the act’s scope.¹³⁶ Similarly, under the “school officials exception,” there is very little criteria needed to meet the qualifications of a school official, making it easy for individuals to receive personal information under this exception.¹³⁷ Zoom is also considered a “school official” for FERPA purposes, allowing the platform to have access to personal student information without needing to gain consent first.¹³⁸

¹³⁴ See *id.* at 468 (noting how there had been a push to update FERPA). See also Sonnemaker, *supra* note 85 (expressing a need to fix FERPA). The cochair of the Parent Coalition for Student Privacy even said,

We really need to fix FERPA . . . It’s a 40-year-old law and it needs to be updated. And it needs to be strengthened so that the onus isn’t on the school district to try to vet and read word for word all these contracts that legal teams for these big edtech companies have put together and each school is on their own.

Id. See also FINAL REPORT, *supra* note 56, at 129 (describing how FERPA was written in 1974 before the existence of the internet). FERPA has “repeatedly been criticized as archaic and [is] in need of updating for the digital age.” *Id.* Some critics think that schools use FERPA “as a shield to hide incriminating or embarrassing information,” due to the confusion surrounding its scope. *Id.*

¹³⁵ See Weinstein, *supra* note 47, at 470 (recognizing that the “health and safety exception” lacks a clear standard that leaves ambiguity as to what can be shared, and the “school officials exception” leaves too much discretion to schools to determine who qualifies as a school official).

¹³⁶ See FINAL REPORT, *supra* note 56, at 131 (highlighting the confusion as to when student information can be shared in preventing emergencies or violence). According to Sonja Trainor, Managing Director for Legal Advocacy at the National School Boards Association, “this confusion . . . creates barriers to information sharing and collaboration, thus hampering the ability to prevent potential acts of violence.” *Id.*

¹³⁷ See SCHOOL RESOURCE OFFICER, *supra* note 56, at 11 (observing that school officials can be a “teacher, school principal, president, chancellor, board member, trustee, registrar, counselor, admissions officer, attorney, accountant, human resources professional, information systems specialist, and support or clerical personnel,” as well as “[c]ontractors, consultants, volunteers, or other third parties to whom a school or district has outsourced certain functions”).

¹³⁸ See *Zoom for K–12*, *supra* note 6 (commenting how Zoom is considered a “school official” for FERPA purposes). Because Zoom is classified as a school official, it

The exceptions weaken FERPA as a whole, allowing student records to be more accessible and lose a sense of privacy as new technological means, such as Zoom, are used to record student behavior.¹³⁹

Since FERPA includes any records that are directly related to a student, Zoom recordings should fall under this category and receive protection.¹⁴⁰ In order for information to fall under FERPA's protection, the information needs to directly relate to a student, their education, and be maintained by the school as an education record.¹⁴¹ Previously, a student captured in the background of an image was not considered protectable student information for FERPA purposes, but it should be due to the capability of advancing technology to use AI data to identify a person under these circumstances.¹⁴² Student information collected from Zoom use, even if the student is not the

can receive Student User personal information because Zoom is performing a service that furthers a "legitimate educational interest." *Id.* According to the Privacy Statement, "Zoom maintains Student User personal information on behalf of, and at the direction of, the School Subscriber and does not use the Student User personal information for other purposes except as permitted by applicable law, including FERPA." *Id.*

¹³⁹ See Weinstein, *supra* note 47, at 473 (describing that while the exceptions are important, they have weakened FERPA "to the point that it is practically useless and merely a protective cover for schools to avoid liability."). While FERPA was once a law that aimed at protecting the privacy of student records, law enforcement and school officials can now use the exceptions to their advantage and use new technological means to retrieve more previously private student data. *Id.* at 473–74.

¹⁴⁰ See *id.* at 466 (recognizing that photos and recordings fall under what is protected in a student's education record, as well as any "personally identifiable information"). See also *FERPA Guide*, *supra* note 81 (highlighting that educational records can include "[v]ideo recordings/streams, chat logs, transcripts, and other information collected or maintained by a School Subscriber while using Zoom's services"); Schwartz, *supra* note 85 (questioning what counts as directly related). According to the U.S. Department of Education, "directly related" can include, but is not limited to, "grades, transcripts, class lists, student course schedules, health records, and student discipline files." Schwartz, *supra* note 85.

¹⁴¹ See Rhoades, *supra* note 48, at 460–61 (observing that FERPA attempts to limit "school disclosure policies to information directly linked to a student, related to their education, and maintained by the school as an education record.").

¹⁴² See *id.* (noting that a student's image captured incidentally or as part of the background is not considered to be directly related to the student for FERPA purposes). However, with EdTech tools, online applications can use machine learning and AI algorithms to identify individuals in the background or tag the image's geolocation to expose the child's location. *Id.* at 461–62. Due to this ability of technology to personally identify the student, "FERPA's guidelines to determine direct linkage to a student in traditional media are incompatible with the enormous capabilities of online applications." *Id.* at 462.

main speaker but rather in the background of the video recording, is directly related to the student because their name identifies them in connection to their video which is often required to be on at the teacher's request.¹⁴³ In terms of the information needing to be related to the student's education to be FERPA protected, the legislature likely did not consider the vast amount of information that could be received from online educational services, creating a need to broaden what is considered an educational record for it to be protected.¹⁴⁴ Since Zoom has the capability to collect personal data depending on how the schools configure the students' Zoom accounts, the legislature should consider what constitutes "related to a student's record" in this digital age.¹⁴⁵ Lastly, the school needs to maintain the information as an educational record for it to fall under FERPA's protection, and even if an EdTech company claims it is holding information as an agent for the school, it usually fails to meet the burden of proving its intent to hold the data as a permanent record.¹⁴⁶ Due to the fact that Zoom states

¹⁴³ See Johnson, *On or off?*, *supra* note 7 (recognizing that some teachers require students to have their video camera on during virtual learning).

¹⁴⁴ See Rhoades, *supra* note 48, at 462 (observing that some "EdTech companies' capability to capture and generate new types of data is testing the limits of educational context required under FERPA."). Under FERPA, only information related to a student's education is protected, but online applications use by schools collect a vast amount of data that schools were not able to consider previously due to technological advancements. *Id.* at 462–63.

¹⁴⁵ See *id.* at 463 (highlighting how "[t]he indirect and inferred data EdTech applications collect often exceeds the traditional [personally identifiable information] found within the permanent student file directly maintained by the school."). "[M]any online applications retain information generated from online messaging, file sharing, and email communication between users." *Id.* See also *Zoom for K–12*, *supra* note 6 (detailing what personal information Zoom can access). "Depending on how the School Subscriber configures its K–12 Account, Zoom may receive personal information contained in 'Customer Content.' Customer Content is any data a K–12 Account User uploads to the Zoom communication platform connected with use of the Service." *Id.* Some examples include meeting hosts or co-hosts recording meetings locally or to Zoom's cloud, K–12 Account Users displaying or uploading information that may be seen by other users of that K–12 Account, allowing meeting participants to share files, allowing hosts or co-hosts to create meeting transcripts, and allowing meeting participants to communicate in-meeting through chat and creating chat logs. *Id.* This "Customer Content may include personal information that is part of an 'educational record' as defined by FERPA." *Id.*

¹⁴⁶ See Rhoades, *supra* note 48, at 463–64 (noting that the Department of Education "requires documents to be maintained and stored by a school, or its agent to be

it only maintains user information for as long as the account is active, it does not appear that the company intends to hold it as a permanent record, showing how it is critical that FERPA is amended to protect this information.¹⁴⁷

Schools are using what occurs over Zoom, and other virtual platforms, to suspend and discipline children; thus, FERPA should protect and seal these recordings and require parental permission to disclose.¹⁴⁸ Due to the classification of names and images that appear on Zoom and other virtual platforms as “personally identifiable information” subject to FERPA considerations, schools should have considered the repercussions that could occur from using Zoom in this virtual learning setting and pushed the government to expand FERPA to include virtual learning.¹⁴⁹ Schools should encourage the legislature to account for advancing technology since the enactment of FERPA

regulated by FERPA,” and “schools must demonstrate the file was retained with some degree of permanency to be considered an education record, such as retaining the record in a filing cabinet or permanent secure database.”). While EdTech companies collect the information as agents for the school, they must also prove there is an intent to hold it as a permanent student record in order for it to be considered protected. *Id.* at 464. If it is only meant to be temporarily held by the EdTech company, it is outside FERPA’s scope. *Id.*

¹⁴⁷ See *Zoom for K–12*, *supra* note 6 (highlighting that “Zoom retains K–12 Account Users’ and Student Users’ personal information for as long as necessary to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for fraud prevention purposes.”); *FERPA Guide*, *supra* note 81 (observing when Zoom retains user information). According to the Guide, Zoom retains

student [personally identifiable information] only for as long as necessary to comply with legal obligations after account termination. Customer content stored on the Zoom Cloud is retained for the life of the account; however, School Subscribers are free [to] delete this content at any time. After an account is terminated, customer content is automatically deleted in accordance with Zoom’s policies and agreements with School Subscribers.

FERPA Guide, *supra* note 81.

¹⁴⁸ See Feis, *supra* note 4 (noting how a boy was suspended when a teacher reported he was playing with a toy gun in his virtual class).

¹⁴⁹ See Johnson, *On or off?*, *supra* note 7 (noting how FERPA is applicable to virtual learning because it is considered personally identifiable information).

and amend the act to account for virtual learning in this new digital era.¹⁵⁰

V. Conclusion

While it is imperative that students continue to learn during the pandemic, K–12 public schools should not be utilizing Zoom without FERPA clarifying and updating how student records are protected with advancing technology. Through the use of Zoom in schools, the government is entering the private homes of students and their families. The legislature must take this into consideration and implement standards for the scope of student privacy and how these digital educational records will be protected. Schools should not be allowed to suspend students for playing with toys within the confines of their own private home, and the best way to outline how schools should treat these matters is through federal legislation. If the government neglects to enact this necessary federal legislation, students’ privacy rights will continue to be invaded in this virtual era because there are no laws that regulate the extent of school intrusion.

¹⁵⁰ See FINAL REPORT, *supra* note 56, at 133 (recommending that the U.S. Department of Education “should work with Congress to modernize FERPA to account for changes in technology since its enactment”).