DE-ESCALATING 'DATAVEILLANCE' IN SCHOOLS

Technologies meant to promote student safety may also invade their privacy and treat them as threats to be managed, rather than learners to be cared for.

By T. Philip Nichols & Alexander Monea

If the transformations in K-12 education over the last two decades had to be encapsulated in a single phrase, "data-driven" would surely be a top contender. Policies like the No Child Left Behind Act inaugurated a vast infrastructure for collecting and analyzing data, and the Every Student Succeeds Act (2015) charged all educators to be facilitators of "data-based instructional decision making" (p. 295). At the same time, technologies for data collection became more sophisticated. New devices and apps have made it easy to amass more, and more kinds of, data about students. Over time, this information has been used to not only document young people's academic progress but also, increasingly, mine for insights into factors that could influence their learning.

School safety has been one prime focus for data-driven interventions. A thriving market has emerged for technologies that monitor students' behavior and alert educators at the earliest signs of trouble. These technologies range from the mundane (e.g., software that notifies administrators when certain websites or keywords are used on school computers) to the highly specialized (e.g., microphones that sweep classrooms for sounds associated with stress, fear, or anger). Such technologies are based on a shared belief: With enough data, we can identify and mitigate threats to school safety, perhaps even before they materialize.

The comfort this belief offers comes at a cost, however. Such technologies are expensive, and there is growing evidence that they don't always work as promised — or, in some cases, at all (Casella, 2018; Gillum & Kao, 2019). In addition, many of these technologies subject young people to invasive forms of data-driven surveillance — or *dataveillance* (van Dijck, 2014) — and thus violate students' privacy and erode trust within school communities. Indeed, educators we've worked with in our research on dataveillance technologies often report feeling uneasy about both the volume of data harvested and the ways this information can position students as potential risks to be managed rather than learners to care for and support.

These concerns raise important questions for educators. How might the sense of security schools derive from dataveillance come at the expense of students' actual well-being and privacy? And what steps could educators take to de-escalate the dependence on such technologies without compromising students' safety?

Who's watching what?

In many ways, surveillance in schools is nothing new. Routine practices like taking attendance, proctoring exams, tracking academic progress, and stationing hall monitors around buildings are

T. PHILIP NICHOLS (Phil_nichols@baylor.edu; @philnichols) is an assistant professor in the Department of Curriculum and Instruction at Baylor University, Waco, TX. He is the author of *Building the Innovation School: Infrastructures for Equity in Today's Classrooms* (Teachers College Press, 2022).
ALEXANDER MONEA (amonea@gmu.edu) is an assistant professor in the Departments of English and Cultural Studies at George Mason University, Fairfax, VA. He is author of *The Digital Closet: How the Internet Became Straight* (MIT Press, 2022).

GETTY IMAGES

For many schools, the possibility of mining data to mitigate safety risks and save educators time and energy is too enchanting to pass up.

all strategies educators use to observe students' behaviors so they can intervene, if necessary. There is also a long history of using technologies to supplement these strategies. A security camera on a closed-circuit television network, for instance, effectively acts as a permanent hall monitor. Likewise, software that offers teachers a real-time view of their class's computer screens functions similarly to a classroom seating arrangement that allows them to look over multiple students' shoulders simultaneously.

These forms of observation, whether mediated by technology or not, are what scholars call *vertical surveillance* (Sewell, 2012). They are vertical because, in each instance, an authority figure — usually a teacher or administrator — is actively watching. Even a security camera, which passively records hours of footage, requires an active onlooker to scroll back through its contents to identify moments of interest — say, a student skipping class or an altercation in the hallway. In vertical surveillance, a person must analyze, interpret, and act on any observations.

Today's dataveillance technologies are somewhat different. Rather than relying on educators to observe or interpret students' behaviors, these technologies make their own determinations about what activities merit attention. They absorb vast amounts of data, analyze it for usable insights, and then push out these judgments for teachers and administrators to use. In this sense, they are a kind of *horizontal surveillance*. Where previously a teacher might vertically surveil their classroom by looking around to determine whether students seem engaged, a dataveillance technology might use facial-recognition software to identify those whose expressions it interprets as "disengaged" and notify the instructor.

While both vertical and horizontal surveillance involve gathering and using data to inform decisions, educators have a different relationship to the data in each. In vertical surveillance, teachers identify what's relevant from the data. In horizontal surveillance, algorithms reduce, sort, and classify data and pass assessments on to teachers. Dataveillance, in other words, inserts an additional layer of decision making between teachers and the information they use to guide their practice. Rather than making decisions about data, they are reacting to a technology's interpretations of data.

In highlighting these differences, we don't mean to suggest that one always is better than another. Without careful and continuous reflection, any surveillance — horizontal or vertical, high tech or low tech — can damage community trust and student well-being. But understanding these distinctions helps us also understand the appeal of dataveillance technologies and the potential implications of bringing them into schools.

The data imperative

Some teachers may feel uneasy about the layer of automated decision making that horizontal surveillance adds to their classrooms. For many, however, the additional distance between educators and raw data is what makes dataveillance alluring.

Vertical surveillance, even when aided by technology, is bounded by the limits of time and attention. Exam proctors and security cameras can miss activities that occur just out of their view, and overworked teachers can struggle to track each student's individual progress every day. Horizontal surveillance is premised on the idea that, with enough data, these limits can be overcome. By using automation, dataveillance dramatically increases the volume of data that can be collected and used in schools. This, advocates suggest, frees teachers to direct their attention toward the most pressing classroom concerns, including some that may have gone undetected with vertical observation alone.

This promise drives the development and adoption of security-oriented educational technologies today. For many schools, the possibility of mining data to mitigate safety risks and save educators time and energy is too enchanting to pass up. This enchantment, in turn, creates a demand for technology providers to package more intensive dataveillance features into their products. What results is a cycle scholars have called the *data imperative* (Fourcade & Healy, 2017) — where the perceived benefits of collecting some data are used to justify the collection of more data, and so on.

We've seen this cycle in our own research on device management software. One of the most ubiquitous school security technologies, device management software, monitors the use of school-issued devices, like laptops and tablets. GoGuardian, the most popular of these services, currently tracks the digital activities of more than 25 million students and 500,000 teachers in more than 10,000 schools (Anand & Bergen, 2021). Significantly, when these technologies were first introduced a decade ago, they were

marketed as tools for locating lost computers, pushing out software updates, and blocking unauthorized content. Over time, however, their ambitions have escalated. GoGuardian and its competitors, like Securly and Gaggle, now also advertise themselves as vital resources for anticipating safety risks related to suicide, self-harm, bullying, and school violence.

The data imperative helps explain the shift in these companies' aspirations. In 2016, GoGuardian made headlines when a California school used one of its incident reports to intervene after a student was found searching for terms associated with self-harm (Kamenetz, 2016). This led to speculation that, with more data, schools might be able to preempt other safety risks. Shortly after, GoGuardian launched Beacon, a service that scrapes students' search terms, browsing history, social media pages, and chats and alerts school officials about data it links to sexual content, self-harm, or bullying. Since then, GoGuardian and its competitors have continued developing new dataveillance features to one-up each other's offerings. Securly, for instance, uses "sentiment analysis" to identify angry or fearful tones in students' messages that could indicate psychological distress. Likewise, with the COVID-19 pandemic, almost all these services now extend their horizontal surveillance to home computers.

The risky business of dataveillance

Stepping back, it's not difficult to see the ethical dilemma the data imperative poses for schools. When educators believe student safety is on the line, there is virtually no limit to the kinds of data collection they would be willing to authorize. Moreover, even if the resulting blanket of horizontal surveillance never identifies potential dangers, this absence of security issues can provide a peace of mind that validates the decision to continue using dataveillance technologies. Once schools are caught in the data imperative's cycle, it's difficult to de-escalate.

The biggest winners in this arrangement are the companies that sell dataveillance technologies. They make up an important sector in a rapidly growing $3 billion school security industry (Keierleber, 2018), in part, because their businesses capitalize on educators' desire to mitigate risk at all costs. These companies appear to be well aware of the hold they have on schools. Part of GoGuardian and Gaggle's sales pitch to educators is that they have prevented dozens of troublesome incidents from occurring. Even though journalists have never been able to verify such claims (Feathers, 2019), the possibility alone is persuasive enough for many schools.

Yet the comfort these companies market to schools can, at times, paper over the significant limitations of dataveillance technologies and the risks that they can introduce into classrooms.

Limited evidence of effectiveness

First, there is little evidence that dataveillance technologies actually make students safer. Despite the lofty claims in their marketing materials, their "success stories" are almost exclusively anecdotes about hypothetical what-ifs, and the evidence from actual use in schools points to significant inaccuracies in their judgments (Gillum & Kao, 2019; Pangrazio et al., 2022). Our own research on educators' uses of device management software affirms these findings. While many teachers we've spoken with are generally optimistic about the potential benefits of such technologies, their actual experiences have been less rosy. Our interviews are filled with accounts of overzealous filters that flood inboxes with incident reports, prevent classes from accessing basic resources, and mistakenly target students (and teachers) as potential threats.

The impacts of these shortcomings don't fall evenly on all students. Because dataveillance technologies can inherit race, class, and gender biases from their creators (Benjamin, 2019), school dataveillance can disproportionately affect students from marginalized communities. Young people with different home languages or dialects, for instance, can be unfairly flagged by over-sensitive content sensors. Likewise, LGBTQ+ students, many of whom are likely to seek identity-affirming resources online (Trevor Project, 2019), can be discouraged from doing so either by site restrictions or the knowledge that they are being monitored (Monea, 2022). For many students, then, dataveillance can be detrimental to their safety.

Erosion of trust

Second, dataveillance technologies erode trust in communities. The layer of automated decision making that dataveillance adds to classrooms distances teachers not just from the raw data, but also from the students about whom data are collected. In our research, we often hear administrators lament that the hours spent following up on automated incident reports cuts into their time for developing connections with students or facilitating community-building experiences.

This works in the other direction as well. Researchers have shown that intensive surveillance makes young people feel singled-out and scrutinized, even when they have done nothing wrong; one consequence of this is that it makes them less

trusting of the teachers or authority figures who they associate with these forms of surveillance (Livingstone, Stoilova, & Nandagiri, 2019). By positioning students as potential threats to be monitored, rather than learners to support, dataveillance technologies can work against the best intentions of educators to nurture caring communities in their schools.

Violations of privacy

Finally, dataveillance technologies heighten risks for privacy violations. Because of the data imperative, the speed at which new dataveillance technologies are entering classrooms has outpaced schools' abilities to keep up with privacy concerns. In our research, we've found that districts often have rudimentary guidelines to protect students' personal information (e.g., names, addresses, demographic details), but the volume and variety of data now being collected poses more serious risks than these policies often realize.

For instance, large pools of student and teacher data — browsing history, search terms, personal chats, geolocations — take on new, ominous potentials at a moment when state legislatures are stripping protections for LGBTQ+ communities, policing access to health services, and threatening the jobs of those who teach about systemic racism. This is especially concerning because the data harvested in classrooms rarely resides in schools but is funneled back to the developers of dataveillance technologies, who may have different standards for privacy than educators or families (Garcia & Nichols, 2021).

"I consolidated my overdue book fines and student lunch debt into one easy monthly payment."

How to break the cycle

In light of dataveillance's shortcomings, educators face a crucial question: How might we break the data imperative's cycle and de-escalate our dependence on these technologies? While there is no simple or singular answer, we can take steps to better align our relationships to data and surveillance with our larger commitment to the safety of our students and communities.

Prioritize student safety over risk management

A first step involves disentangling our assumptions about safety and risk. Dataveillance technologies make a comforting promise that using data to identify and mitigate risks will make students safe. The trouble is the process for gathering and acting on this data often introduces new and unanticipated risks into classrooms. Efforts to preempt hypothetical dangers can easily create viscerally real ones. For this reason, we need to prioritize the actual safety and well-being of students over our desire to predict or manage potential risks.

One important way to do this is to pay particular attention to who might be inordinately impacted by efforts to keep schools safe. There are long histories of both vertical and horizontal surveillance practices that have unfairly targeted and disciplined students from marginalized communities. Recognizing and redressing these legacies — for instance, by choosing not to collect data that could be weaponized against minoritized students — are foundational for building safer and more caring schools for everyone.

Develop data policies within the community

Too often, school policies related to student data and privacy are made in isolation from the people who must live with their consequences. In our research, we found that school and district technology policies often originated from a singular administrator (e.g., an IT coordinator) and tended to focus on narrow data protections and expectations for appropriate technology use. For example, they may focus on preventing hackers from gaining access to school databases, but they rarely focus on what data service providers like GoGuardian should be able to access or whether all collectable data ought to be harvested, stored, and shared with school administrators. While protecting schools from outside security threats is important, these policies miss an opportunity to articulate a bold, collective vision for the kind of relationship a given community wishes to have with data technologies.

A step toward such a vision could include hosting discussions with students, teachers, and families about their concerns and desires related to data

collection, surveillance, and safety. These conversations might then lead to the development of shared norms and standards, which educators could use to assess how well new devices, apps, and products and their use align with the interests and priorities of the larger community.

Deviate from default settings

A final step involves recognizing that educational technologies don't need to be adopted wholesale. Developers of dataveillance technologies often bundle their products with additional features, hoping educators will use them and become loyal to their brand. When GoGuardian introduced its Beacon software, for instance, it came packaged with its standard device management software. But just because a feature is available, or arrives in schools "activated" as a default setting, doesn't mean schools ought to use it.

Educators should feel empowered to ignore or turn off any features that extend a technology's reach deeper into their classrooms than necessary. In our research, we have seen districts successfully strong-arm technology providers into fundamentally changing data practices and product functions by threatening to not renew contracts. Such negotiations are especially effective when administrators can present companies with community-generated norms and standards that providers must meet. While such tactics aren't always successful, they move educators from accepting technologies as they are to advocating for those that will best support the needs and safety of students. Schools have significantly more leverage in making such demands than they realize.

Prioritizing well-being

If the last two decades are any indicator, the push for data-driven education isn't going anywhere. The data imperative appears poised to continue escalating the surveillance of students' behavior, academic performance, and even their emotional states. However, this escalation is not inevitable. By prioritizing the well-being of school communities over the mitigation of risk, we can begin to articulate an alternate vision for data, surveillance, and safety — one that takes, as its starting point, a commitment to the flourishing of all students. ■

References

Anand, P. & Bergen, M. (2021). *Big teacher is watching: How AI spyware took over schools.* Bloomberg.

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity Press.

Casella, R. (2018). School security and its corporate offerings. In J. Deakin, E. Taylor, & A. Kupchik (Eds.), *The Palgrave international handbook of school discipline, surveillance, and social control* (pp. 389-404). Palgrave Macmillan.

Every Student Succeeds Act, 114-95 U.S.C. (2015).

Feathers, T. (2019). Schools spy on kids to prevent shootings, but there is no evidence it works. *Vice*.

Fourcade, M. & Healy, K. (2017). Seeing like a market. *Socio-Economic Review, 15* (1), 9-29.

Garcia, A. & Nichols, T.P. (2021). Digital platforms aren't mere tools — they're complex environments. *Phi Delta Kappan, 102* (6), 14-19.

Gillum, J. & Kao, J. (2019). Aggression detectors: The unproven, invasive surveillance technology schools are using to monitor students. *ProPublica*.

Kamenetz, A. (2016). *Software flags suicidal students, presenting privacy dilemma*. NPR.

Keierleber, M. (2018, August 9). Inside the $3 billion school security industry. *The 74 Million*.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. Research Findings*. London School of Economics and Political Science.

Monea, A. (2022). *The digital closet: How the internet became straight*. MIT Press.

Pangrazio, L., Stornaiuolo, A., Nichols, T.P., Garcia, A., & Philip, T. (2022). Datafication meets platformization: Materializing data processes in teaching and learning. *Harvard Educational Review, 92* (2), 257-283.

Sewell, G. (2012). Organization, employees, and surveillance. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 303-313). Routledge.

Trevor Project. (2019). *National survey on LGBTQ mental health*. Author.

van Dijck, J. (2014). Datafication, dataism, and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society, 12* (2), 197-208.