JUST CITIES TOOLKIT

Education Technology

MARCH 8, 2022

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

This is a guide to evaluating so-called "smart cities" technology for local advocates, community members, and elected officials. Cities' technology decisions frequently ignore the interests of impacted and marginalized communities, eroding democratic norms, public trust, civil rights, and even public safety. This guide provides a framework and language for advocating for *just* cities rather than smart cities. Use the following portion of the guide to evaluate technology and municipal data collection at schools and universities.

I. Introduction

Educational technology (EdTech) is a $3.2 billion[i] industry domestically, up from $1.45 billion[ii] in 2015 and poised to grow by $87 billion[iii] worldwide in the next ten years. Even before the pandemic forced schools everywhere online, 95% of all teachers used technology in the classroom on a daily basis.[iv] We use "EdTech" broadly to encompass all forms of technology in school environments, from online proctoring services and learning management systems to student monitoring software and school security cameras. Even before EdTech's rapid expansion, many tools were deployed opaquely without teacher training, equity and privacy assessments, or community engagement. We introduce design principles to help policymakers and advocates evaluate and regulate the use of EdTech in their schools.

EdTech needs these local checks. The field is largely underregulated, especially at the national level. The 1974 Family Educational Rights and Privacy Act (FERPA) is decades out of date and unable to address novel technologies.[v] Rather that insisting on additional scrutiny, states have done the opposite, reducing regulations or even encouraging[vi] or mandating the technology.[vii] As a result, schools are rushing to adopt EdTech without evidence it *should* be adopted.[viii] Our framework suggests the reverse. Given EdTech's documented harms, the technology must be subjected to rigorous scrutiny at every stage of acquisition, maintenance, and use, and retained only where its benefits are independently verified and its harms are non-discriminatory.

II. Design Principles

1. **Preventing police cooption**
2. **Establish educational need**
3. **Equity**
4. **Community engagement**
5. **Transparency**
6. **3rd party reviews, audits, and grievance processes**
7. **Wholistic budgeting**
8. **Data minimization**
9. **Equitable privacy protection**
10. **Expanded EdTech oversight**

1. Preventing Police Cooption

Under the American legal system, every municipal data system is a policing tool in the making. Our default standard is to allow police to access any type of EdTech data with (at most) a court order. In the absence of technical, legal, and political safeguards against police cooption of smart cities education systems, EdTech should be evaluated under the more searching framework put forward for smart cities police technology. The remainder of this toolkit only applies where a city has created sufficient safeguards that the public can rest assured that the relevant technology will be used solely for its intended educational purpose.

Key safeguards can include:

- A ban on any use of student data for non-education purposes;
- A warrant requirement for use of such data for non-education purposes;
- Data destruction practices that effectively prevent use of the data for law enforcement purposes.

2. Establish educational need

Any EdTech purchase or deployment must start with the question: "What need does this tool serve?" EdTech vendors have an interest in framing their systems as valuable to your school district, but that's frequently not the case. At worst, the technology harms students needlessly: online proctoring software, for example, subjects students to surveillance without any documented benefit.[ix] Even where EdTech can provide *some* benefit, schools must evaluate whether there are less expensive, less intrusive alternatives that better advance a school's educational priorities.

3. Equity

Even where EdTech meets a need, it should be rejected when a tool's harms fall disproportionately on BIPOC students, low-income students, immigrants, or other historically marginalized groups. This risk is present with all EdTech, but it is particularly acute for tools that collect data of interest to police and immigration agencies and for artificial intelligence systems. Tools and their privacy policies should be scrutinized for inequitable impacts: systems ranging from AI academic advising,[x] to remote proctoring,[xi] to student admissions algorithms have all demonstrated racial and gender bias, and lax privacy policies can disproportionately harm students from overpoliced communities. Ablest EdTech systems frequently exclude visually impaired and hearing-impaired students and students with movement disorders. Vendors typically place the burden on students to flag accessibility issues and to test and identify adequate alternative tools or arrangements.[xii] Prior to deploying any EdTech system with the potential to discriminate, schools should require an equity assessment including a contextual analysis of how such a system will work in a particular community, since even seemingly unbiased tools can augment existing forms of inequality.

4. Community engagement

Tools should not be procured without community support. Schools should engage the community to assess an EdTech tool's possible harms and, positively, to determine whether a tool is appropriate and helpful for affected student populations. For community members to give meaningful feedback on a tool, decisionmakers must provide relevant information, observing the transparency principle and making third-party reviews and audits public (more below). Tools should not be retained without consulting students, parents, and teachers: community members should play a part in tools' periodic reviews to ensure that decisionmakers know how tools are used and experienced by students and teachers.

5. Transparency

As just discussed, the community should participate in decisions to acquire new EdTech—giving notice is an inadequate approach to transparency. Once acquired, schools and universities should publicly report the EdTech vendors and tools they use along with detailed, plain-language explanations of how data is collected, stored, shared, and accessed. Schools should reject contract provisions that would prevent them from disclosing these details. Moreover, schools should publicly post all contracts they enter with EdTech vendors. While many states require some disclosures from public K-12 schools, the laws currently vary in the level of disclosure that is required.[xiii] Private schools and universities should adopt these same privacy practices.

Currently, parents, advocates and policymakers generally don't know enough about how EdTech is used in our local communities and across the country. Reviews and audits should be public, reasonably brief (or contain summaries), and should be written in nontechnical language that is accessible to parents and teachers. Vendors' secrecy typically inhibits both parental choice and meaningful oversight from elected officials. Stakeholders should reject any EdTech tool whose vendor refuses to rigorously disclose all data collection practices and features. Schools should also insist on affirmative consent from vendors to engage in software audits, as detailed below. Schools should always publicly disclose data breaches and attacks on their systems.

6. Third-party reviews, audits, and grievance processes

Many EdTech vendors sell products based on claims that are unsupported by independent research. While some technologies can provide real benefits, a vendor's assertion should always be substantiated by independent, third-party review of the relevant product. Such a review should answer a standard set of questions that establish the tool's educational value and reveal the vendor's data security and data privacy practices. As discussed above, tools should not be acquired without an equity assessment conducted by a disinterested third party. Free or donated EdTech should not be used without meeting the same or similar standards.

Once in use in a school, EdTech should be subject to periodic reviews, audits, and a grievance process. Reviews incorporating feedback of teachers and students using a tool should be used to periodically check the tool's pedagogical utility, its privacy and security practices, its equity impact, and how tools are actually being used in the classroom. Software audits, conducted as needed, can assess privacy and

security questions in more detail. Schools should also consider implementing a formalized complaint process to allow students and teachers to play a role in documenting any harms caused by EdTech.

7. Wholistic budgeting

EdTech offloads labor onto educators, who are forced to not only navigate new systems, but to interpret a deluge of data. When systems flag "suspicious behavior" on tests or claim a student is in need of support, it is schools that have to perform quality checks, reviewing the automated decisions for mistakes.[xiv] Many educators have been forced to adopt new EdTech tools without adequate support, imposing a hidden labor cost on schools as countless hours are diverted from other tasks. EdTech purchase plans should include a clear training and labor budget, outlining an evidence-based estimate of the time and resources needed for teachers to learn to use new tools, plus the resources needed to monitor educators' actual use of EdTech. Purchase plans should also outline the opportunity costs associated with EdTech compared to non-technology alternatives.

8. Data minimization

Many EdTech products capture more data than is needed to carry out the function they seek to complete, increasing the risk of harm to students if their data falls into the hands of police, immigration agencies, or hackers. EdTech products should only collect the data that is necessary to serve their stated educational objective. Once data is captured, it should only be retained as long as is absolutely necessary, with clear access controls and parameters on use. When excessive detailed data is captured and preserved by EdTech, it becomes a target for parties with unrelated, non-educational goals. Vendors may also find a market for such data. EdTech creates the most acute concerns when it records students' location history, biometric data, communications content, and private residences.

9. Equitable privacy protection

EdTech can pose a particularly acute risk for marginalized and multi-marginalized students. Location history data[xv] that might seem innocuous for some students can pose an acute threat to those who are undocumented or have criminal justice involvement.[xvi] Students with low socioeconomic status may be more reliant on school-provided devices as their sole source of internet connectivity; if schools install content monitoring software on those devices, they violate these students' privacy.[xvii] Schools should set EdTech policies that center the experience of students most impacted by EdTech harms. Because teachers may adopt EdTech tools in their classrooms without prior approval, teacher training should reinforce a culture of respect for students' privacy and emphasize the importance of scrutinizing EdTech tools with risks to students in mind.

10. Expanded EdTech oversight

Schools should articulate a structure for making decisions about EdTech and student data collection. This structure should identify decisionmakers and lay out processes for making decisions around EdTech, reviewing those decisions, terminating contracts, and retaining and disposing of student data. Elected officials at the local, state, and federal level need to actively review the data provided by schools and universities on the real-world performance of EdTech. Even where a vendor has a

product that appears promising on paper, the lived experience of such technology in the classroom can vary considerably. Officials must actively solicit feedback on EdTech systems from a broad cross section of educators and teachers, identifying potential harms and unexpected costs. Every EdTech system should be reevaluated at least once a year and discontinued immediately where it fails to demonstrate a positive net impact. The massive economic and labor investment being made in EdTech requires a proportional level of oversight.

III. Selected EdTech Use Cases

Facial Scanning and Identification/Authentication/Recognition

Facial scanning refers to any forms of technology that can recognize the human face. This technology can supposedly verify identities for tests, parse through a database of other faces to produce a match, or monitor students' facial behaviors, such as their eye movements.[xviii]

Facial recognition simply does not work. On top of consistently failing to identify non-white persons,[xix] facial recognition fails at higher rates for children than for adults, which makes school-deployment of the technology suspect.[xx] It does not serve any educational need.

Room Scanning

Room scanning refers to technologies that require students to show their surroundings to a third party (usually a proctor) via web camera to ensure that nothing objectionable is present.

Room scanning is not equitable because it is not accessible. Vision-impaired students and others often struggle to scan their room to the standards the software stipulates.[xxi] But even if room scanning could be made accessible, it would still be objectionably invasive. Lower-income students can be effectively punished for the lack of a private bedroom or office.

Flagging

Flagging occurs when either a person or an algorithm registers a supposedly anomalous student behavior and flags it as a potential instance of cheating or other behavior needing attention.

Flagging poses equity concerns. Because algorithms designed to detect misconduct look for anomalous behaviors, they will always flag non-normative behaviors despite these behaviors being normal for people with disabilities.[xxii] When software stores video data for later review, it memorializes a student's likeness and surroundings in a digital record. This data is particularly vulnerable in the case of data breaches,[xxiii] and students often have no knowledge of either their rights over the footage or who can access it.

Spending on flagging tools diverts schools' limited resources away from superior alternatives. For example, self-harm monitoring software claims to gather data about students from their online activities to flag students deemed at risk.[xxiv] Software is likely a poor replacement for robust mental health services that the technology may displace in a school budget. Similarly, acquiring a technological

tool to help students meet their IEP goals can divert resources away from hiring special education educators.

Other decision-making algorithms

Decision-making algorithms are pieces of software that make choices about students. These choices can be as seemingly innocuous as suggesting courses for next term[xxv] to choosing which students the police will surveil.[xxvi]

Algorithms are often opaque, whether by design or due to vendor secrecy, so that students do not know what produced the automated decisions that concern them. When based on machine learning, they may reproduce the race and gender bias of their training data.[xxvii] Without more information about such tools, including the ability to audit their software, schools can only hope to avoid harming students.

Dark Patterns

Dark patterns are design choices that "nudge" or manipulate users into making particular decisions.[xxviii] For example, dark patterns can gamify homework so that students spend more time learning geometry.

Dark patterns pose enormous transparency concerns. Their very name suggests that the manner they use to frame choices is intentionally deceptive. While such tools might lead students to spend more time studying math, their deceptive nature means that users do not know what is happening. Without third party reviews, audits, and grievance processes, the tools may engage in problematic practices unseen.

Electronic Student Monitoring

Electronic student monitoring denotes any form of surveillance that tracks student behavior on the internet in both school and non-school settings. Examples include social media monitoring,[xxix] self-harm monitoring,[xxx] and content-based interaction monitoring.[xxxi]

Broad monitoring of general student internet activity, such as schools examining social media posts, is profoundly invasive. Such data collection does not serve any particular educational need and violates the principle of data minimization. Even more limited monitoring of student activity during school can create a chilling effect on student expression, where students believe they must actively self-censor.[xxxii] Monitoring students creates an exploitable trove of sensitive student data.

IV. Partners and Resources

ACLU Washington, "Algorithmic Equity Toolkit"
https://www.aclu-wa.org/AEKit

Commonsense Media, "The Common Sense Census: Inside the 21st-Century Classroom"
https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-educator-census-inside-the-21st-century-classroom_1.pdf
A survey of educational technology in K-12 classrooms across the US.

The Consortium for School Networking (CoSN)
https://www.cosn.org/about/
Resources for vetting technology for K-12 decisionmakers. Student privacy page at
https://www.cosn.org/edtech-topics/student-data-privacy/

The EdTech Equity Project, "School Procurement Guide: Buying Edtech Products with Racial Equity in Mind"
https://coda.io/d/School-Procurement-Guide_dYBoc7ujwQA/School-Procurement-Guide_su9mx#_luXPB

New America, "The Promise and Peril of Predictive Analytics in Higher Education"
https://www.newamerica.org/education-policy/policy-papers/promise-and-peril-predictive-analytics-higher-education/

OECD, "Children in the digital environment: Revised typology of risks."
https://www.oecd.org/digital/children-in-the-digital-environment-9b8f222e-en.htm

Student Data Privacy Consortium, "Standard Student Data Privacy Agreement"
https://sdpc.a4l.org/agreements/FINAL_SDPC_NDPA_V1-4.pdf

Student Privacy Compass:
"Reopening Schools During the COVID-19 Pandemic: Issue Briefs"
https://studentprivacycompass.org/resource/reopening-schools-during-the-covid-19-pandemic-issue-briefs/
Overview of student data privacy as it relates to EdTech adopted widely during the COVID-19 pandemic.

"The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies: Recommendations for Schools"
https://studentprivacycompass.org/resource/self-harm-monitoring/

"Student Privacy Primer"
https://studentprivacycompass.org/resource/student-privacy-primer/

"State Student Privacy Laws"

https://studentprivacycompass.org/state-laws/

---

[i] "U.S. Edtech Roars with Over $3.2 Billion Invested in First Half of 2021" (Reach Capital), July 15, 2021, https://medium.com/reach-capital/u-s-edtech-roars-with-over-3-2-billion-invested-in-first-half-of-2021-d69049dbce30.
[ii] Michael Winters, "Christmas Bonus! US Edtech Sets Record With $1.45 Billion Raised in 2015," EdSurge News, December 21, 2015, https://www.edsurge.com/news/2015-12-21-christmas-bonus-us-edtech-sets-record-with-1-85-billion-raised-in-2015.
[iii]"Global EdTech Funding 2021 - Half Year Update" (HolonIQ), June 28, 2021, https://www.holoniq.com/notes/global-edtech-funding-2021-half-year-update/.
[iv] David Nagel. "How Teachers Use Technology in the Classroom," *THE Journal*, May 18, 2019, https://thejournal.com/articles/2019/05/08/how-teachers-use-technology-in-the-classroom.aspx.
[v] Charley Locke, "What Would Proposed Changes to FERPA Mean for Edtech?" Edsurge News, April 14, 2015. https://www.edsurge.com/news/2015-04-14-what-would-proposed-changes-to-ferpa-mean-for-edtech.
[vi] "Implementation of Cameras in the Classroom" (New Jersey Education Association), August 25, 2020, https://www.njea.org/implementation-of-cameras-in-the-classroom/.
[vii] "Long-Range Plan for Technology 2006-2020" (Educational Technology Advisory Committee), November 2006, https://tea.texas.gov/sites/default/files/FinalCombinedLRPT2020.pdf.
[viii] Noel Enyedy, "Personalized Instruction: New Interest, Old Rhetoric, Limited Results, and the Need for a New Direction for Computer-Mediated Learning," November 24, 2014, https://nepc.colorado.edu/publication/personalized-instruction.
[ix] Albert Fox Cahn et al., "Snooping Where We Sleep: The Invasiveness and Bias of Remote Proctoring Services" (Surveillance Technology Oversight Project, November 11, 2020), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/5fd78bac79515d2e1fde4bb7/1607961518518/Snooping+Where+We+Sleep+Final.pdf.
[x] Todd Feathers, "Major Universities Are Using Race as a 'High Impact Predictor' of Student Success," *The Markup*, March 2, 2021, https://themarkup.org/news/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success.
[xi] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR, 77–91, 2018. https://proceedings.mlr.press/v81/buolamwini18a.html.
[xii] Lydia X. Z. Brown, "How Automated Test Proctoring Software Discriminates Against Disabled Students" (Center for Democracy and Technology), November 26, 2020, https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/.
[xiii] "State Student Privacy Laws," Student Privacy Compass, accessed October 15, 2021, https://studentprivacycompass.org/state-laws/.
[xiv] Colleen Flaherty, "Big Proctor," Inside Higher Ed, May 11, 2020, https://www.insidehighered.com/news/2020/05/11/online-proctoring-surging-during-covid-19.
[xv] Gennie Gebhart, "Spying on Students: School-Issued Devices and Student Privacy" (Electronic Frontier Foundation, April 13, 2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy.
[xvi] Rani Molla, "Law Enforcement Is Now Buying Cellphone Location Data from Marketers," Vox, February 7, 2020, https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration.
[xvii] L. Holden Williams, "Student Activity Monitoring Software and the Risks to Privacy" (Center for Democracy & Technology, October 6, 2021), https://cdt.org/insights/student-activity-monitoring-software-and-the-risks-to-privacy/.
[xviii] Cahn, Snooping Where We Sleep.
[xix] Tom Simonite, "The Best Algorithms Still Struggle to Recognize Black Faces," Wired, accessed October 13, 2021. https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.
[xx] Nishra Srinivas, Karl Ricanek, Dana Michalski, David Bolme, and Michael King, "Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults," June 1, 2019, https://www.osti.gov/biblio/1559665.
[xxi] Nora Caplan-Bricker, "Is Online Test-Monitoring Here to Stay?" The New Yorker, May 27, 2021. https://www.newyorker.com/tech/annals-of-technology/is-online-test-monitoring-here-to-stay.
[xxii] Flaherty, Big Proctor.
[xxiii] Errick, Kirsten, "Students Sue Online Exam Proctoring Service ProctorU for Biometrics Violations Following Data Breach," Law Street Media, March 15, 2021, https://lawstreetmedia.com/news/tech/students-sue-online-exam-proctoring-service-proctoru-for-biometrics-violations-following-data-breach/.
[xxi] Amelia Vance, Sara Collins, Jasmine Park, Anisha Reddy, and Yasamin Sharifi, "The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies," Student Privacy Compass, September 27, 2021, https://studentprivacycompass.org/resource/self-harm-monitoring/.
[xxiv] Amelia Vance, Sara Collins, Jasmine Park, Anisha Reddy, and Yasamin Sharifi, "The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies," Student Privacy Compass, September 27, 2021, https://studentprivacycompass.org/resource/self-harm-monitoring/.

[xxv] Cynthia Hubert, "Hornet Launch Scheduling Takes Hold with Incoming Freshmen," accessed October 13, 2021, https://www.csus.edu/news/articles/2020/6/12/New-freshmen-embrace-strategic-scheduling.shtml.
[xxvi] Neil Bedi and Kathleen McGrory, "Pasco's Sheriff Uses Grades and Abuse Histories to Secretly Label Kids Potential Criminals," November 19, 2020, https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data.
[xxvii] Andre M Perry and Nicol Turner Lee, "AI Is Coming to Schools, and If We're Not Careful, so Will Its Biases," *Brookings*, September 26, 2019, https://www.brookings.edu/blog/the-avenue/2019/09/26/ai-is-coming-to-schools-and-if-were-not-careful-so-will-its-biases/.
[xxviii] Natasha Singer, "When Websites Won't Take No for an Answer," The New York Times, May 14, 2016, https://www.nytimes.com/2016/05/15/technology/personaltech/when-websites-wont-take-no-for-an-answer.html.
[xxix] Aaron Leibowitz, "Could Monitoring Students on Social Media Stop the Next School Shooting?" The New York Times, September 6, 2018, https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html.
[xxx] Vance, "Self-Harm Monitoring Technologies."
[xxxi] Hugh Grant-Chapman, Elizabeth Laird, and Cody Venzke, "Student Activity Monitoring Software: Research Insights and Recommendations" (Center for Democracy & Technology), September 21, 2021, https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations/.
[xxxii] Grant-Chapman, "Student Activity Monitoring Software."

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT