NEPC
NATIONAL EDUCATION POLICY CENTER

Thursday, April 9, 2020

Newsletter

Children's Data Privacy During COVID-19 Closures: 10 Questions To Ask

With nearly every American school shut down to slow the spread of COVID-19, many educators are either adopting online educational and conferencing products for the first time or, at the very least, increasing their use of these resources. This means that millions of children per day are logging in from home to Internet communications platforms such as Zoom, Google's G-Suite for Education, Nearpod, and Flipgrid. These online options offer the potential for students to connect with their classmates and teachers, structure their days at home, and "save" some of the remaining school year. But they also pose threats to students' privacy.

Students from high-risk populations (such as undocumented families, foster youth, or survivors of domestic violence) may face immediate threats to their safety as a result of videos, images, or other information about them shared online. All students face longer-term threats, as education software collects information about them, both with and without their knowledge. Some of this information, including educational records transferred from a child's school or a video that includes a child's name, is explicitly personally identifiable.

Other information, such as de-identified clickstream data, cannot be used to identify the child—at least in theory. In reality, de-identified data are easily re-identified and also may provide sufficiently significant details about a child's online choices and activities that make knowing the child's actual identity superfluous. Companies with access to such information may use it alone or in combination with other available data for a variety of purposes that parents have not necessarily approved. These activities may lead to targeting marketing to children and their families, limiting their access to information or opportunities, or propagating misinformation.

Even if companies do not use it for ill, the information is vulnerable to theft. In September

2018, the Federal Bureau of Investigation (FBI) warned that the "widespread collection of sensitive information by EdTech could present unique exploitation opportunities for criminals," including identity theft, harassment, and extortion. Effective data security practices are thus essential to prevent crimes that are facilitated by the collection and storage of data from children.

For these reasons, many parents and educators are concerned about how ed-tech companies are collecting and protecting students' data. Given the current circumstances, they may not want to, or may feel unable to, challenge the move to online schooling. However, adults concerned about children's privacy can still help guide their schools and districts by asking school officials and companies critical questions about how their children's data are being collected, safeguarded, and used.

Here are some questions to ask:

1. What procedures does the school have in place to inform parents about the educational technology products their children are asked to use, including which data each product collects, stores, and uses from students? For example, some state laws require schools to provide this information to parents on the school websites.

2. What procedures does the school have in place to obtain parental consent for their children to use education technology products? Companies (for example, Google, Zoom, and Summit Learning) often contract directly with schools, and these schools then provide consent on behalf of parents. Federal law requires parental consent if a company intends to use or disclose children's personal information for its own commercial purposes in addition to its provision of services to the school. In February 2020, the state of New Mexico filed a suit against Google for, among other things, preempting parents' legal right to consent for their children.

3. May I examine the privacy policy and terms of service for educational technology products the school is requiring students to use? Sometimes privacy policies are posted online, but a 2019 National Education Policy Center research brief by Faith Boninger, Alex Molnar, and Christopher Saldaña (University of Colorado Boulder) found that some companies do not make privacy policies publicly available. For example, Schoolnet, a Pearson product that collects and maintains data on student assessments, negotiates privacy policies individually with districts. If state law does not require schools to post the contracts they sign on their website, concerned parents or educators must obtain their policy from their district.

4. What data do the companies supplying the education technology products collect from students? Which items are considered "personally identifiable information (PII)?" The U.S. Department of Education defines PII as including "information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information." State and federal student privacy laws focus on PII, and typically allow schools to release "de-identified" student data without parental consent. Parents can advocate for their districts to limit the sharing of de-identified data, which contains significant information about students.

5. Does the company have access to students' education records, in addition to any data their product may collect? If a company is designated as a "school official" (as Google is when the school uses G Suite for Education), federal law permits schools to transfer education records (e.g., transcripts, health records) to it without parental consent. Parents can encourage their districts to negotiate contracts that limit companies' access to education records.

6. For what purposes does the company collect each piece of data from students? Some state laws require schools to provide this information on their websites. In the absence of such a requirement, schools and districts can demand this information from companies.

7. Are the purposes for which the company collects data for the direct benefit of students? Many state student privacy laws allow companies to use students' personally identifiable information (PII) to develop and improve their products. Such exemptions may be legal, but they have little, if any, benefit for the students whose data are being used.

8. Which data are shared with additional ("third-party") companies? What are the names of those companies? For what purposes are the data shared with them? Products often rely on third-party providers to help provide their services. Those companies also have access to student data.

9. What procedures does the company have in place to protect data it collects from students? Do security procedures conform to rigorous cybersecurity frameworks, such as National Institute of Standards and Technology (NIST) or the Federal Risk and Authorization Management Program (FedRAMP)? "Industry standards" often referred to in privacy policies are not actual standards.

10. What options does the school provide for students and families who do not want to use online educational technology products? Parents with legitimate concerns about privacy or safety should request reasonable alternatives from their schools, and encourage their schools to provide them.

Although schools are moving to online options out of a perception of necessity right now, we can expect a full-funded advocacy push from them to continue to use them going forward. Now is a very good time to demand satisfactory answers to hard questions that will help schools and districts obtain important information and concessions from the companies with which they contract, and make better choices about the products they require their students to use.

Additional Resources:

1. NEPC's Commercialism in Education Research Unit has published several research briefs examining the student privacy concerns presented by education technology products.

2. The Parent Coalition for Student Privacy offers toolkits for student and teacher privacy, and information about how to talk to schools about their contracts with Google.

3. The Campaign for Commercial-Free Childhood offers a Screens in Schools Action Kit containing resources for how to talk to schools about their use of online educational technology products.

4. The Network for Public Education published a guide for parents about online learning.

5. The Electronic Frontier Foundation published a report on student privacy issues presented by school-issued devices.

6. Colorín Colorado provides resources related to privacy considerations for English Language Learners.

NEPC Resources on Virtual Education

This newsletter is made possible in part by support provided by the Great Lakes Center for Education Research and Practice: http://www.greatlakescenter.org

The National Education Policy Center (NEPC), a university research center housed at the University of Colorado Boulder School of Education, produces and disseminates high-quality, peer-reviewed research to inform education policy discussions. Visit us at: http://nepc.edu