The Legal Intelligencer

Privacy and Security Considerations in the Era of Remote Learning

As a result of COVID-19, people across the country have been forced to continue their educational endeavors from the confines of their homes. Students are now being engaged from home for everything from school, dance lessons, craft videos and cooking classes.

By **Jennifer J. Daniels, Jeffrey N. Rosenthal and David J. Oberly** | July 17, 2020

Jennifer Daniels, Jeffrey Rosenthal and David Oberly of Blank Rome (Photo: Courtesy Photo)

As a result of COVID-19, people across the country have been forced to continue their educational endeavors from the confines of their homes. Students are now being engaged from home for everything from school, dance lessons, craft videos and cooking classes.

Importantly, distance-learning arrangements often involve the collection and use of the personal information about children. Organizations offering distance learning opportunities need to consider their privacy and security obligations under a patchwork of federal and state laws—as well as how they can satisfy said obligations given the slim privacy/security assurances received from online service providers.

Legal Landscape

A variety of laws may impact educational organizations that offer distance learning opportunities; which law(s) apply may depend on factors such as whether the educational organization is a school, whether a school is for profit or not for profit, the age of the child, the state where the child resides, and the mechanism through which the information is collected.

COPPA: Any website or online service collecting personally identifiable information (PII) from children under 13 must comply with the Children's Online Privacy Protection Act (COPPA). COPPA imposes privacy and security requirements on operators of commercial websites and online services. COPPA is comprised of two core requirements: supplying privacy notices detailing the operator's data practices; and obtaining verifiable parental consent. These requirements are imposed on the website or operator of the online service collecting PII from the child. The online service or website will often look to pass along the obligation to provide notice and obtain verifiable parental consent to the educational organization.

COPPA permits schools to provide consent directly to educational technology (i.e., ed tech) vendors if the vendor satisfies the following requirements: provides the school with a COPPA-compliant notice of its data practices; and limits the use of children's PII solely for a school-authorized educational purpose, and refrains from commercial uses of such data.

FERPA: The Family Educational Rights and Privacy Act (FERPA) only applies to schools that receive federal education funding. FERPA requires schools to obtain written parental consent to disclose the education records of any student under 18. Under FERPA, "education records" are records that are: directly related to a student; and maintained by the school or a party acting on its behalf.

FERPA permits schools to use video conferencing apps and other technology for remote learning under the "school official" exception to FERPA's consent requirements, provided the outside vendor: performs a service for which the school would otherwise use its own employees; satisfies the school's criteria for being a school official with a legitimate educational interest in the educational records; remains under the direct control of the school; and (4) uses education records only for authorized purposes.

State Laws: Organizations must also be aware of state laws, which vary widely from one state to another. For schools, many state-level student privacy laws impose broader and more stringent requirements than FERPA. For example, the New York Department of Education (NYDE) now requires schools to post a "parents bill of rights for data privacy and security" that complies with NYDE requirements. The California Consumer Privacy Act (CCPA) applies to for-profit educational organizations that meet the size thresholds to fall within the scope of the law. The CCPA gives California residents broad new rights with respect to their personal information, including rights to transparency, access, and deletion. Minors also have the right to consent before their personal information is disclosed to a third party in what is considered a "sale" under the CCPA.

Online Terms of Service and Privacy Policies

Educational organizations must also consider the terms of service (TOS) and privacy policies maintained by third-party vendors.

For example, the TOS for the popular online video conferencing product, Zoom states that although it is a covered operator subject to COPPA, it maintains no responsibility for obtaining parental consent, leaving that for schools to handle. Further, the Zoom TOS provides that the service is not intended for use by individuals under the age of 16, unless it is through an educational account held by a school subscriber. Unless an organization pays for an educational account, Zoom's terms of service prohibits minors under the age of 16 from having an account or using the services.

Key Privacy and Security Considerations

To provide students with the ability to continue learning outside the classroom, while at the same time maintaining compliance with the law, educational organizations should consider the following:

- **Transparency:** To promote transparency, educational organizations should ensure students and parents are informed regarding: the terms of service offered by ed tech vendors; privacy notices provided by ed tech vendors, including any COPPA notice or online privacy policy; a description of student PII shared with vendors; and a list of the online services to which consent has been provided on behalf of the parent.

- **Consent:** Online service providers should be requiring verifiable parental consent, consistent with COPPA, before allowing an account to be established for a child under the age of 13. Consent may be required under FERPA if the online service provider intends to use personal information in "education records" for purposes like the site's own analytics or advertising. In some cases, it may not be clear that COPPA or FERPA apply, but it is still a best practice to obtain parental consent to uses and disclosures of personal information about a minor.

- **Nonstudent Observation:** Consider how to handle non-students, such as siblings or visitors, that may observe remote learning sessions. In general, educational organizations should discourage non-students from observing remote learning sessions to avoid potential privacy issues.

- **Recording and Sharing:** Where a live session is recorded and made available to other students, the educational organization must consider how this impacts the privacy of any student that participated in the live session. Educational organizations should avoid recording online sessions involving students whenever possible. Instead, consider having teachers pre-record their lessons without students present to minimize the privacy risks associated with recording live sessions.

- **Remote Meetings/Conferences:** Teachers can conduct remote meetings/conferences with parents/students—but must ensure no PII from the student's education record is overheard or disclosed to any third parties.

- **Student-Created Accounts:** Educational organizations should avoid requiring students to create their own personal accounts for any remote learning activities.

- **Written Contracts:** Educational organizations should enter into written contracts with ed tech vendors whenever possible, such as by including an addendum in its remote learning agreements with vendors that ensures compliance with both federal and state law.

- **Review TOS and Privacy Policies:** Educational institutions should carefully review the TOS and privacy policies of potential vendors to evaluate whether they pose any potential privacy issues. For example, does the privacy policy or TOS explain how the service will comply with COPPA or FERPA? Does the privacy policy say that the service provider will use personal information to target advertisements? Teachers should be instructed to use only those services that have been previously vetted for privacy by the school.

- **Data Security Measures:** Educational institutions should evaluate the security of the services they use to

provide distance learning capabilities. For example, does the service provider encrypt the audio and video of a session? Is end-to-end encryption an option? Are strong passwords required to log into a session? Do recordings of your sessions live on the cloud even after you delete them from your account?

- **Consult Experienced Privacy Counsel:** Finally, schools should consult experienced privacy counsel to ensure its vendors' operations do not run afoul of the school's legal obligations under COPPA, FERPA and other relevant student privacy/security laws.

Conclusion

As the education sector continues to encourage students to learn from home while the COVID-19 public health emergency persists, educational organizations cannot lose sight of the complex web of privacy laws/regulations implicated by remote learning. By considering the issues addressed above—and consulting with experienced privacy counsel—educational institutions can not only ensure compliance in the short-term, but also install a solid foundation to maintain compliance with privacy laws long after the COVID-19 pandemic is in our collective rear-view.

Jennifer J. Daniels *is a partner at Blank Rome and serves as chair of the firm's cybersecurity and data privacy group. She can be reached at daniels@blankrome.com.*

Jeffrey N. Rosenthal *is a partner at the firm. He concentrates his complex litigation practice on consumer and privacy class action defense, and regularly publishes and presents on class action trends, attorney ethics and biometrics. He can be reached at rosenthal-j@blankrome.com.*

David J. Oberly *is an attorney in the Cincinnati office of the firm and is a member of the cybersecurity and data privacy and privacy class action defense groups.His practice encompasses both counseling and advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters, as well as representing clients in the defense of privacy and biometric privacy class action litigation. He can be reached at doberly@blankrome.com.*