July 20, 2020

NYIPLA White Paper
Data Privacy, Copyright Law, and Cybersecurity Issues Related to Distance Learning

About the NYIPLA:

The New York Intellectual Property Law Association ("NYIPLA") is a ninety-eight-year-old bar association with hundreds of attorneys who practice in the areas of patent, copyright, trademark, data privacy, and other intellectual property ("IP") law. It is one of the largest regional IP bar associations in the United States.

As diverse technical and legal specialists, NYIPLA members are well-positioned to provide recommendations about IP law, including data privacy law, and frequently opine on federal and state legislative developments that relate to intellectual property. The NYIPLA is aware that New York's state and local governments will need to address a wide variety of legal issues that will likely touch on intellectual property law as they seek to implement solutions to address the realities of a distance economy, in particular with respect to distance learning. Through this White Paper, the NYIPLA seeks to support New York's efforts during this challenging time by contributing to future decision-making related to issues concerning data privacy, copyright law, and cybersecurity.

I. Data Privacy Concerns Associated with Distance Learning:

Several data privacy laws should be evaluated to ensure that school districts comply with all applicable laws and regulations related to protecting the private information of educators, students, and families. Should New York State choose to implement or even mandate some amount of distance learning for New York schools, any legislation implementing a state-wide distance learning protocol, must also address at least the concepts outlined below.

A. Federal Privacy Laws:

The Federal Educational Rights and Privacy Act ("FERPA") is a federal privacy law that applies to educational agencies and institutions funded by the U.S. Department of Education. *See* 20 U.S.C. § 1232g; 34 CFR Part 99. It provides, among other things, parents and students the right to: (1) access education records and correct records as appropriate; and (2) provide consent to disclosure of personally identifiable information ("PII")[1] from student education records. "Education records" are defined by FERPA as records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution, or by a party acting for the agency or institution. Under FERPA, an educational agency or institution may not disclose PII from a student's education records without prior written consent, unless the disclosure meets an exception.

[1] Personally identifiable information under FERPA has a similar definition under New York State Education law related to data privacy, and includes direct identifiers, such as a student's name or identification number, as well as indirect identifiers such as student's date of birth, or other information which can be used to distinguish or trace an individual's identity, either directly or indirectly through linkages with other information.

In March 2020, the Student Privacy Policy Office ("SPPO") of the U.S. Department of Education released a guidance entitled FERPA and Virtual Learning During COVID-19 in response to questions about available resources on virtual learning and FERPA. *See* https://www.aacrao.org/docs/default-source/covid-19/ferpa-virtual-learning-032020.pdf. One of the key resources mentioned therein, entitled "Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices" addresses privacy and security considerations relating to computer software and other web-based tools used in distance learning. *See* https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best. Notable best practices include creating and following processes for evaluating vendor contracts for privacy and security consideration; implementing written contracts with online education services that help schools and districts maintain the required "direct control" over the use and maintenance of student data; and taking extra precautionary steps when accepting clickwrap licenses for consumer applications. The SPPO also provided model terms of service with providers of online education services in an additional guidance. *See* https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service.

The Children's Online Privacy Protection Act ("COPPA") is a federal privacy law that applies to Internet websites that collect personal information from children under the age of 13. *See* 16 C.F.R. Part 312; 15 U.S.C. §§ 6501-6505. COPPA's definition of personal information is broad and includes "persistent identifiers" such as IP addresses or mobile device IDs. COPPA requires, among other things, that covered websites: (1) post privacy policies describing their collection, use, and disclosure practices related to children's personal information; (2) obtain verifiable parental consent for the collection, use, or disclosure of personal information from children; and (3) provide notice and obtain verifiable parental consent for the use of third-party ad networks or plug-in providers on the website. While COPPA does not have a private cause of action, violations of the Act are "unfair or deceptive" acts or practices in violation of the Federal Trade Commission Act ("FTCA"). As a result, entities that violate COPPA may be subject to Federal Trade Commission ("FTC") enforcement or fines. The FTC permits schools to consent on behalf of parents to the collection of children's personal information by educational technology services. If such consent has been provided, the information may only be used for educational purposes.

In April 2020, the FTC provided guidance on how school districts and educational technology companies can comply with COPPA, in particular with respect to COVID-19. *See* https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus. In its guidance, the FTC explained that schools should provide parents with information about the websites and online services that they will use to collect personal information from children. Schools should also review the privacy and security policies of the educational technology services they employ and gain an understanding of how such services will collect, use, and disclose personal information collected from students.

B. New York State Privacy Laws:

Education Law 2-d ("Ed. Law 2-d") was enacted as part of the New York State budget for the 2014-2015 school year, primarily to protect the PII contained in student records, as well as in principal and educator evaluations. While Ed. Law 2-d had some basic requirements for the protection of PII, it was not until January 2020 that the New York Board of Regents adopted new regulations intended to protect student's and educator's PII in Part 121 of Title 8 of the NYCRR ("Part 121"). The most notable requirements in the regulations concerning Ed. 2-d are:

- the specific clarification that Ed. Law 2-d and the ensuing regulations apply not only to public school districts but to charter schools and State-approved special

education schools (collectively referred to herein as "Schools");

- a requirement that the Parent's Bill of Rights must be included in *every* contract the school has with third-party vendors that receive student, teacher, or principal PII;

- a requirement that all Schools must post information on their websites about the third-party agreements implicating PII that the Schools are a party to; and

- a requirement that by June 2020 all Schools must adopt a policy and privacy plan that aligns with the National Institute for Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Security Version 1.1.

Effectively, these regulations will impact schools and the products many of them rely on to educate children in even the most basic ways. For example, educators will no longer be able to use click wrap programs that collect or use PII with standard "Terms and Conditions." Third-party vendors, regardless of their place of business, must accept the specific requirements of Part 121 if they are to do business with a New York State School. Thus, many programs that Schools rely on now may no longer be available if a vendor does not or cannot comply with the new more stringent version of Part 121.

Additionally, the New York Stop Hacks and Improve Electronic Data ("NY SHIELD Act") was enacted in July 2019 and became effective on a rolling timeline between October 2019 (data breach notification obligations) and March 2020 (requiring cybersecurity safeguards). The Act was promulgated in part as a response to the Equifax breach and an acknowledgement that New York Resident electronic data must be safeguarded in a reasonable and responsible manner. Therefore, anyone who owns or processes New York Resident electronic data must comply with the technical, physical, and administrative safeguards outlined in the act at N.Y. G.B.L § 899-bb. School districts and their vendors must comply with the requirements of the NY SHIELD Act, including the need for an incident response plan that complies with breach notification requirements of the Act.

II. Copyright Issues Associated with Content Use Online:

The New York State Department of Education, School Superintendents, and School District leaders should be mindful of the copyright laws that apply to content generated by educators for online programs. Educators also need to be cognizant of copyright issues associated with the use of content online that was not originated by the educator. Items like articles, songs, and photographs are presumed to be copyrighted, so educators cannot simply post copyrighted materials they find on the Internet to their online classrooms. This is true even if there is not a "©" copyright notice on the materials. Copyright owners have the exclusive right not only to duplicate the works they own, but to distribute and display them. Some types of copyrighted works may be subject to compulsory licenses, such as recorded music, so educators should check with their school administrators or district leaders to find out if they have a license to use recorded music. With respect to other types of materials, educators should make a good faith determination of whether they need a license. The Copyright Clearance Center has good resources available to determine whether an institution-wide license or a pay-per-use license is available for certain types of copyrighted materials frequently used in academia, such as scholarly articles or journals. *See* https://www.copyright.com/.

Notably, there are a lot of misconceptions about when a copyrighted work can be used without license because it is a "fair use." It is not a simple analysis and courts are inconsistent in how they apply the rules. Generally, courts are mandated by copyright statute to apply a 4-part test which includes: (1) the purpose of the use; (2) the amount of the work taken; (3) the type of work it is (*e.g.*, highly creative vs. work of historical facts);

and (4) the impact of the use on the market for the original work. *See* 17 U.S.C. § 107. In particular, the second factor is often misunderstood. There are no clear "rules of thumb," and it is not correct to say (as some believe) that if one uses less than a third of the original work, then it is a fair use. Courts instead emphasize the qualitative nature of what is being used—*i.e.*, is the portion that is being used the "heart" of the original work—rather than a formulaic quantitative percentage. So, while use of copyrighted materials solely for educational purposes is often deemed to be a fair use, if your institution charges a fee for access to the materials, it may need a license, particularly where there is an existing licensing market for the materials you want to use. Thus, it is important to take each factor into account and to make a case-by-case determination in good faith on whether it is necessary to seek a license before using copyrighted materials. It is also important to provide credit to the original author(s) of the work when posting a work online with class materials, irrespective of whether there is a license covering the use or a "fair use"—that is a practice that should always be observed.

III. Cybersecurity Risk Mitigation Efforts during Remote Learning:

To protect the PII exchanged during remote learning and comply with the data privacy regulations listed above, New York State Department of Education, and School District leaders should consider the following cybersecurity risk mitigation efforts that should be implemented:

- **Data encryption** is necessary to protect private information, both at rest (long-term storage) and in transit (in-use and live broadcasts). The State must evaluate whether or not a potential remote-learning platform adequately encrypts user (educator and student) information, such as passwords, personally identifiable information, and the video and audio data, that comprises a remote learning session. This information should be encrypted when stored, when exchanged between the user and the platform, and when the platform allows for direct data streaming between users. Inadequate encryption can lead to sensitive information being exposed to third parties in the event of a breach. Similarly, when a platform serves as an intermediary for data streams between users, a breach in the platform's security can result in the remote learning sessions becoming exposed and recorded.

- **Meeting controls** must be available to teachers and administrators to protect virtual classrooms from unwelcome intrusions. This can mean giving a class administrator the power to limit virtual classroom access and levels of participation. Remote learning platforms must provide the training and default settings required to protect virtual classrooms. The failure to do so can lead to a disruption of a virtual classroom and can create a platform in which a malicious actor has a trapped audience to which the exposure of graphic content cannot be avoided.

- **Proper cyber hygiene** procedures must be in place to ensure the security of a platform from various kinds of attacks. A remote learning platform should have a team dedicated to securing the platform by instituting appropriate business and software development practices, which includes testing for, locating, and remediating security flaws, both in code and in business processes. A failure to follow proper cyber hygiene procedures can result in security breaches that expose sensitive data, as well as creating a vector of attack for the systems belonging to the users.

- **Data breaches** can implicate state notification laws. With each state having its own regulation, and data likely not kept within the state contracting for services, it can become a complicated question of where notice is required

and what occurrences constitute a breach. All remote learning platforms must be capable of prompt legal compliance with all potentially applicable state data breach notification laws.