TO: P-12 Education Committee
FROM: Elizabeth R. Berlin
SUBJECT: Proposed Addition of Part 121 to the Regulations of the Commissioner Relating to Student Data Privacy
DATE: January 3, 2019
AUTHORIZATION(S): 

SUMMARY

Issue for Discussion

Should the Board of Regents add a new Part 121 to the Commissioner's regulations to implement Education Law §2-d relating to protecting personally identifiable information?

Reason(s) for Consideration

Required by State statute - Education Law §2-d as enacted by Chapter 56 of the Laws of 2014.

Proposed Handling

The proposed amendment is presented to the P-12 Education Committee for discussion at the January 2019 Board of Regents meeting. A copy of the proposed amendment is included as Attachment A.

Procedural History

A Notice of Proposed Rule Making will be published in the State Register about January 30, 2019. Supporting materials are available upon request to the Secretary to the Board of Regents.
Background Information

Chapter 56 of the Laws of 2014 added §2-d to the Education Law effective April 2014. The focus of the law is the privacy and security of personally identifiable information (PII) of students, and certain annual professional performance review (APPR) data of teachers and principals. The law outlines certain requirements for educational agencies and their third-party contractors to ensure the security and privacy of such protected information.

Regulatory Background

The proposed amendments to Part 121 of the Commissioner’s regulations were developed in consultation with stakeholders and the public. In 2017, the Chief Privacy Officer created the Data Privacy Advisory Council (DPAC) which consists of members drawn from diverse stakeholder groups and includes parents, industry advocates, administrative and teacher organizations and information technology experts. A list of DPAC members is included as Attachment B. The DPAC created two sub-committees to aid its work: the drafting workgroup and the technical standards workgroup. The drafting workgroup worked on the language of the regulation while the technical standards workgroup (drawn from a cross-section of experts from across the state) was responsible for recommending a standard for educational agency data security and privacy policies and practices. To seek public comments on additional elements of the parent’s bill of rights and the regulation, the Department held fourteen public forums across the state in May and June and solicited for electronic comments during this period. The Chief Privacy Officer also created a Regulation Implementation Workgroup comprised of educational agency stakeholders from the field such as RIC Directors, BOCES staff, district technical directors and other experts in the field to collaborate in the work of developing an implementation roadmap, and other tools and resources to aid the adoption and implementation of the regulation and the data security and privacy standard it adopts. The input received from all stakeholders was critical to developing these regulations.

To highlight some provisions, Part 121 clarifies the data security and privacy obligations of educational agencies and third-party contractors; establishes requirements for contracts and other written agreements where PII will be provided to a third-party contractor and also attempts to clarify obligations where click-through agreements for software applications are utilized; establishes the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the standard for educational agencies data security and privacy programs; directs educational agencies to ensure that all employees that handle PII receive annual data security and privacy training; and requires that educational agencies identify a data protection officer that will be responsible for the educational agency’s data security and privacy program.

Related Regents’ Items

- April 2018 Information Privacy Program Update
**Recommendation**

Not applicable.

**Timetable for Implementation**

Following the 60-day public comment period required under the State Administrative Procedure Act, it is anticipated that the proposed rule will be presented to the Board of Regents for permanent adoption at its May 2019 meeting, and that the proposed amendment will become effective on July 1, 2019.
ATTACHMENT A

AMENDMENT TO THE REGULATIONS OF THE COMMISSIONER OF EDUCATION

Pursuant to Education Law sections 2-d, 101, 207 and 305.

A new Part 121 shall be added, effective July 1, 2019, to read as follows:

Part 121

Protecting Personally Identifiable Information

§121.1 Definitions. As used in this Part, the following terms shall have the following meanings:

(a) *Breach* means the unauthorized access, use, or disclosure of student data and/or teacher or principal data.

(b) *Chief Privacy Officer* means the Chief Privacy Officer appointed by the Commissioner pursuant to Education Law §2-d.

(c) *Commercial or Marketing Purpose* means the sale of student data, or its use or disclosure, whether directly or indirectly, to derive a profit, for advertising purposes or to develop, improve or market products or services to students.

(d) *Contract or other written agreement* means a binding agreement between an educational agency and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

(e) *Disclose or Disclosure* mean to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

(g) Educational Agency means a school district, board of cooperative educational services (BOCES), school, or the Department.

(h) Eligible Student means a student who is eighteen years or older.

(i) FERPA means the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

(j) NIST Cybersecurity Framework means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

(k) Parent means a parent, legal guardian, or person in parental relation to a student.

(l) Personally Identifiable Information, as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232-g, and as applied to teacher and principal data, means personally identifying information as such term is defined in Education Law §3012-c(10).

(m) Release shall have the same meaning as Disclosure or Disclose.

(n) School means any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, an approved provider of preschool special education, any other publicly
funded pre-kindergarten program, a school serving children in a special act school
district as defined in Education Law §4001, an approved private school for the
education of students with disabilities, a State-supported school subject to the
provisions of Article 85 of the Education Law, or a State-operated school subject to the
provisions of Articles 87 or 88 of the Education Law.

(o)  **Student** means any person attending or seeking to enroll in an educational
agency.

(p)  **Student Data** means personally identifiable information from the student
records of an educational agency.

(q)  **Teacher or Principal Data** means personally identifiable information from
the records of an educational agency relating to the annual professional performance
reviews of classroom teachers or principals that is confidential and not subject to
release under the provisions of Education Law §§3012-c and 3012-d.

(r)  **Third-Party Contractor** means any person or entity, other than an
educational agency, that receives student data or teacher or principal data from an
educational agency pursuant to a contract or other written agreement for purposes of
providing services to such educational agency, including but not limited to data
management or storage services, conducting studies for or on behalf of such
educational agency, or audit or evaluation of publicly funded programs. Such term shall
include an educational partnership organization that receives student and/or teacher or
principal data from a school district to carry out its responsibilities pursuant to Education
Law §211-e and is not an educational agency, and a not-for-profit corporation or other
nonprofit organization, other than an educational agency.
Unauthorized Release means any release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

§121.2 Educational Agency Data Collection Transparency and Restrictions.

(a) Educational agencies shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(b) Each educational agency shall take steps to minimize its collection, processing and transmission of personally identifiable information.

(c) Each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with federal and state law and the educational agency's data security and privacy policy.

§121.3 Parents Bill of Rights for Data Privacy and Security.

(a) Each educational agency shall publish on its website a parent’s bill of rights for data privacy and security (“parent’s bill of rights”) that complies with the provisions of Education Law §2-d (3).
The parent’s bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information.

Each educational agency shall include with its parent’s bill of rights supplemental information for each contract the educational agency enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data. The supplemental information must be developed by the educational agency and include the following information:

1. the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
2. how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);
3. the duration of the contract, including the contract’s expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., if, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).
4. if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. where the student data or teacher or principal data will be stored.

described in such a manner as to protect data security, and the security protections
taken to ensure such data will be protected (e.g., offsite storage, using a cloud service provider); and

(6) address encryption of the data as provided in Education Law §2-d 5(f)(5).

(d) Each educational agency shall publish on its website the supplement to the parent's bill of rights for any contract or other written agreement with a third-party contractor that will receive personally identifiable information, provided that each such supplement may be redacted to the extent necessary to safeguard the privacy and/or security of the educational agency's data and/or technology infrastructure.

§121.4 Parent Complaints of Breach or Unauthorized Release of Personally Identifiable Information

(a) Each educational agency must establish and communicate to parents and eligible students its procedures for parents and eligible students to file complaints about breaches or unauthorized releases of student data.

(b) The complaint procedures must require educational agencies to promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect any personally identifiable information.

(c) Following its investigation, the educational agency shall provide the parent or eligible student with a report of its findings within a reasonable period but no more than 30 calendar days from receipt of such complaint by the educational agency. In extenuating circumstances, where the educational agency requires additional time to investigate the complaint or cooperate with law enforcement, or where releasing the report may compromise security or impede the investigation of the incident, the
educational agency shall provide the parent or eligible student with a written explanation
that includes the approximate date when the educational agency anticipates that the
report will be released.

(d) Educational agencies must maintain a record of all complaints of breaches
or unauthorized releases of student data and their disposition in accordance with
applicable data retention policies, including the Records Retention and Disposition
Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

§121.5 Data Security and Privacy Standard.

(a) As required by Education Law §2-d (5), the Department adopts the
National Institute for Standards and Technology Framework for Improving Critical
Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF)
as the standard for data security and privacy for educational agencies.

(b) No later than December 31, 2019, each educational agency shall adopt
and publish a data security and privacy policy that implements the requirements of this
Part and aligns with the NIST CSF.

(c) Each educational agency’s data security and privacy policy must also
address the data privacy protections set forth in Education Law §2-d (5)(b)(1) and (2as
follows:

(1) every use of personally identifiable information by the educational agency
shall benefit students and the educational agency (e.g., improve academic
achievement, empower parents and students with information, and/or advance efficient
and effective school operations).

10
(2) personally identifiable information shall not be included in public reports or other documents.

(d) An educational agency’s data security and privacy policy shall include all the protections afforded to parents or eligible students, where applicable, under FERPA and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), and the federal regulations implementing such statutes.

(e) Each educational agency must publish its data security and privacy policy on its website and provide notice of the policy to all its officers and employees.

§121.6 Data Security and Privacy Plan.

(a) Each educational agency that enters into a contract with a third-party contractor shall ensure that such contract includes a data security and privacy plan. The data security and privacy plan must:

(1) outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency’s data security and privacy policy;

(2) include a signed copy of the parent privacy bill of rights;

(3) include a requirement that any officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access; and

(4) comply with Education Law §2-d.
§121.7 Training for Educational Agency Employees.

Educational agencies shall annually provide information privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training may be delivered using online training tools and may be included as part of training the educational agency already offers to its workforce.

§121.8 Educational Agency Data Protection Officer

Each educational agency shall designate one or more employees to serve as the educational agency’s data protection officer(s) to be responsible for the implementation of the policies and procedures required in Education Law §2-d and this Part, and to serve as the point of contact for data security and privacy for the educational agency. Such officer(s) must have the appropriate knowledge, training and experience to administer the functions described in this part. This requirement may be fulfilled by a current employee(s) of the educational agency who may perform this function in addition to other job responsibilities.

§121.9 Third Party Contractors

(a) In addition to all other requirements for third-party contractors set forth in this Part, each third-party contractor that will receive student data or teacher or principal data shall:
adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework; comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law § 2-d; and this Part.

(2) limit access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

(3) not use the personally identifiable information for any purpose not explicitly authorized in its contract;

(4) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency, not disclose any personally identifiable information to any other party:
  (i) without the prior written consent of the parent or eligible student; or
  (ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

(5) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody as prescribed by state and federal law, regulations and its contract with the educational agency;

(6) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using controls as specified by the Secretary of the United
States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5; and

(7) not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(b) Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

§121.10 Reports and Notifications of Breach and Unauthorized Release

(a) Third-party contractors shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after such discovery of such breach.

(b) Each educational agency shall in turn notify the Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor’s notification in a format prescribed by the Department.

(c) Third-party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

(d) Educational agencies shall report every discovery or report of a breach or unauthorized release of student or teacher data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.
Educational agencies shall notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 14 calendar days after the discovery of a breach or unauthorized release by an educational agency or the receipt of a notification of a breach or unauthorized release from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of personal information by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the educational agency shall notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor shall pay for or promptly reimburse the educational agency for the full cost of such notification.

Notifications required by this section shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency’s investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.
(h) Notification must be directly provided to the affected parent, eligible student, teacher or principal by first-class mail to their last known address; by email; or by telephone.

(i) Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer shall report such breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

§121.11 Third Party Contractor Civil Penalties

(a) Each breach or unauthorized release of student data or teacher or principal data by a third-party contractor shall be punishable by a civil penalty of the greater of $5,000 or up to $10 per student, teacher, and principal whose data was released, provided that the latter amount shall not exceed the maximum penalty imposed under General Business Law §899-aa (6) (a).

(b) The Chief Privacy Officer shall investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may involve visit to, or examination and inspection of the third-party contractor’s facilities and records by the Chief Privacy Officer.

(c) Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive such data in violation of applicable state or
federal law, the data and security policies of the educational agency, and/or any binding
contractual obligations, the Chief Privacy Officer shall notify the third-party contractor of
such finding and give the third-party contractor no more than 30 days to submit a written
response.

(d) If after reviewing the third-party contractor’s written response, the Chief
Privacy Officer determines the incident to be a violation of the Education Law §2-d, the
Chief Privacy Officer shall be authorized to:

(1) order the third-party contractor be precluded from accessing personally
identifiable information from the affected educational agency for a fixed period of up to
five years; and/or

(2) order that a third-party contractor or assignee who knowingly or recklessly
allowed for the breach or unauthorized release of student data or teacher or principal
data be precluded from accessing student data or teacher or principal data from any
educational agency in the state for a fixed period of up to five years; and/or

(3) order that a third party contractor who knowingly or recklessly allowed for
the breach or unauthorized release of student data or teacher or principal data shall not
be deemed a responsible bidder or offeror on any contract with an educational agency
that involves the sharing of student data or teacher or principal data, as applicable for
purposes of the provisions of General Municipal Law §103 or State Finance Law
§163(10)(c), as applicable, for a fixed period of up to five years;

(4) require the third-party contractor to provide additional training governing
confidentiality of student data and/or teacher or principal data to all its officers and
employees with reasonable access to such data and certify that it has been performed,
at the contractor’s expense. Such additional training must be performed immediately
and include a review of federal and state laws, rules, regulations, including Education Law §2-d and this Part.

(e) If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence, the Commissioner may determine that no penalty be issued upon the third-party contractor.

§121.12 Right of Parents and Eligible Students to Inspect and Review Students Education Records

(a) Consistent with the obligations of the educational agency under FERPA, parents and eligible students shall have the right to inspect and review a student’s education record by making a request directly to the educational agency in a manner prescribed by the educational agency.

(b) An educational agency shall ensure that only authorized individuals gain access to student data. To that end, educational agencies shall require identification or verification of the identity of the parent or eligible student who requested access to an education record.

(c) Requests by a parent or eligible student for access to a student’s education records must be directed to an educational agency and not to a third-party contractor.

(d) Educational agencies are required to notify parents annually of their right to request to inspect and review their child’s education record including any student
data stored or maintained by an educational agency. A notice issued by an educational agency to comply with the FERPA annual notice requirement shall be deemed to satisfy this requirement. Two separate annual notices shall not be required.

(e) Educational agencies shall comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

(f) Educational agencies may provide the records to a parent or eligible student electronically, if the parent consents to such a delivery method. The educational agency must transmit the personally identifiable information in a way that complies with State and federal law and regulations. Safeguards associated with industry standards and best practices, including but not limited to, encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

§121.13 Chief Privacy Officer's Powers
The Chief Privacy Officer shall have the power to access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by an educational agency that relate to student data or teacher or principal data, which shall include but not be limited to records related to any technology product or service that will be utilized to store and/or process personally identifiable information. Based upon a review of such records, the Chief Privacy Officer may require an educational agency to act to ensure that personally identifiable information is protected in
accordance with state and federal law and regulations, including but not limited to
requiring an educational agency to perform a privacy and security risk assessment.

§ 121.14 Severability.

If any provision of this part or its application to any person or circumstances is
adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or
impair the validity of the other provisions of the article or their application to other
persons and circumstances, and those remaining provisions shall not be affected but
shall remain in full force and effect.
## Data Privacy Advisory Council Membership
(as of 12/2018)

<table>
<thead>
<tr>
<th>Name</th>
<th>Title and Position</th>
<th>Organization/Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heather Adams</td>
<td>Assistant in Research and Educational Services</td>
<td>New York State United Teachers</td>
</tr>
<tr>
<td>Tope Akinyemi</td>
<td>Chief Privacy Officer</td>
<td>New York State Education Department</td>
</tr>
<tr>
<td>Georgia Asciutto</td>
<td>Executive Director</td>
<td>Big 5</td>
</tr>
<tr>
<td>Joseph Baranello</td>
<td>Chief Privacy Officer</td>
<td>Office of the General Counsel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New York City Department of Education</td>
</tr>
<tr>
<td>Kyle Belokopitsky</td>
<td>Executive Director</td>
<td>New York State Parent Teacher Association</td>
</tr>
<tr>
<td>Alison Bianchi</td>
<td>General Counsel</td>
<td>New York State Education Department</td>
</tr>
<tr>
<td>Kevin Casey</td>
<td>Executive Director</td>
<td>School Administrators Association of NYS</td>
</tr>
<tr>
<td>Charles Dedrick</td>
<td>Executive Director</td>
<td>New York State Council of School Superintendents</td>
</tr>
<tr>
<td>Jolene DiBrango</td>
<td>Executive Vice President</td>
<td>New York State United Teachers</td>
</tr>
<tr>
<td>Tracy Falvo</td>
<td>Director of Technology</td>
<td>Burnt Hills-Ballston Lake Central School District</td>
</tr>
<tr>
<td>Joseph E. Fitzgerald</td>
<td>Assistant Director</td>
<td>Lower Hudson Regional Information Center</td>
</tr>
<tr>
<td>David Gee</td>
<td>Technology Director</td>
<td>Fox Lane Middle School</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bedford Central School District</td>
</tr>
<tr>
<td>Leonie Haimson</td>
<td>Executive Director</td>
<td>Class Size Matters</td>
</tr>
<tr>
<td>Beth Haroules</td>
<td>Senior Staff Attorney</td>
<td>New York Civil Liberities Union</td>
</tr>
<tr>
<td>Rose LeRoy</td>
<td>Director of Educational Data and Research</td>
<td>New York State Education Department</td>
</tr>
<tr>
<td></td>
<td>P12 Instructional Support</td>
<td></td>
</tr>
<tr>
<td>Dr. Patrick McGrath</td>
<td>Superintendent of Schools</td>
<td>Burnt Hills-Ballston Lake Central School District</td>
</tr>
<tr>
<td>Lisa Rudley</td>
<td>Steering Committee Member</td>
<td>NYS Allies for Public Education</td>
</tr>
<tr>
<td>Julie Shaw, Esq.</td>
<td>Partner</td>
<td>Shaw, Perelson, May &amp; Lambert</td>
</tr>
<tr>
<td>Colleen Sloan</td>
<td>General Counsel</td>
<td>Erie 1 BOCES</td>
</tr>
<tr>
<td>Amelia Vance</td>
<td>Policy Counsel</td>
<td>Future of Privacy Forum</td>
</tr>
<tr>
<td>Jay Worona</td>
<td>General Counsel</td>
<td>New York State School Board Association</td>
</tr>
</tbody>
</table>