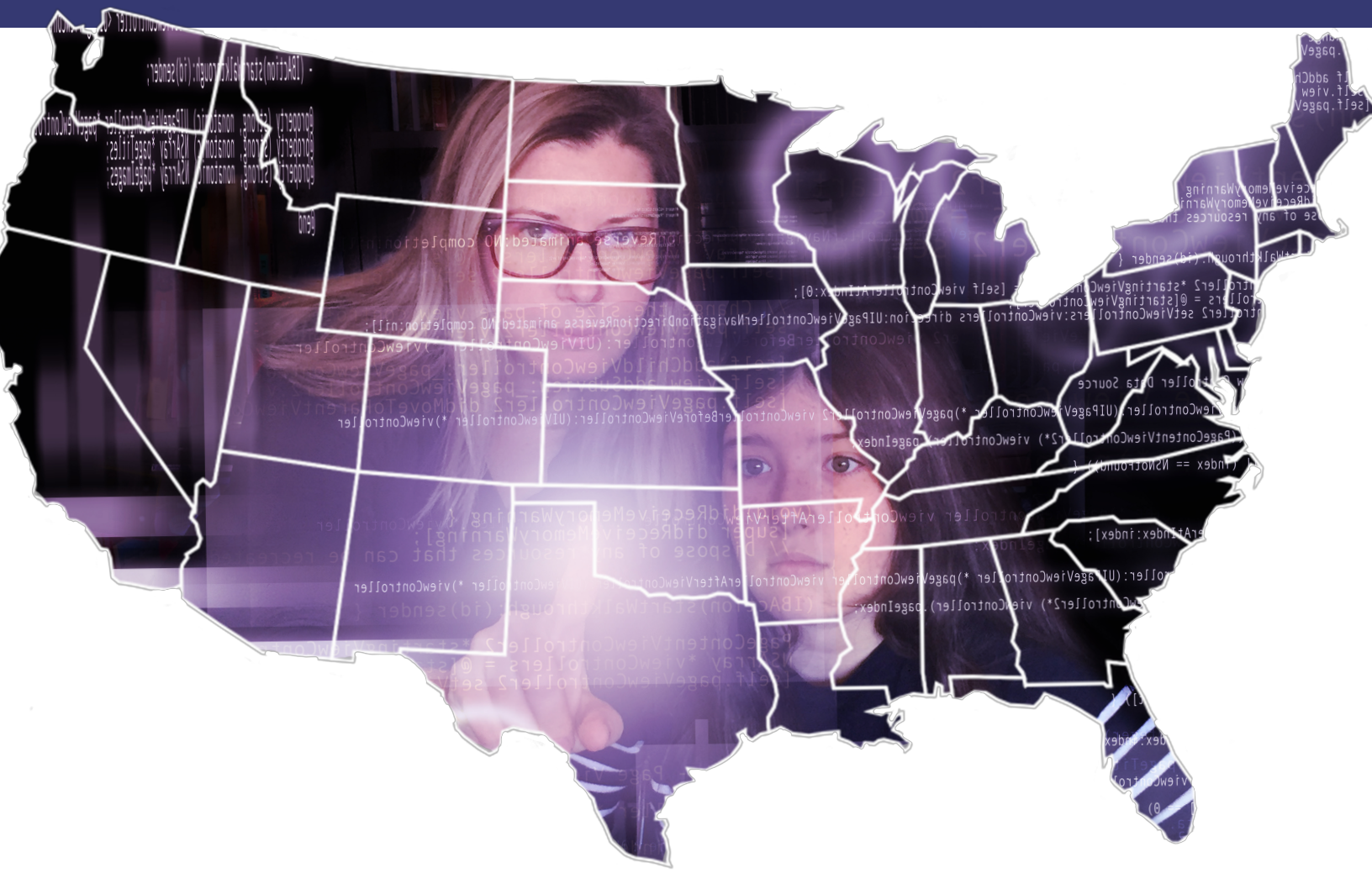
THE STATE STUDENT PRIVACY REPORT CARD TECHNICAL APPENDIX

GRADING THE STATES ON PROTECTING STUDENT DATA PRIVACY



JANUARY 2019

PARENT COALITION FOR STUDENT PRIVACY

THE NETWORK FOR PUBLIC EDUCATION

TABLE OF CONTENTS

Figures

Definitions

Definitions of relevant terms for each law can be found in the comparison matrix. This section is provided for reference and comparison only; no points were awarded. Definitions are organized as follows:

1. Definitions clarifying or expanding on the *Family Educational Rights and Privacy Act's (FERPA)* definition of "personally identifiable information" or the *California Student Online Personal Information Protection Act's (SOPIPA)* definition of "covered information."
2. Relevant definitions of "vendor," "operator," "online service provider," or similar third parties that may collect or receive student information.
3. Definitions of "targeted advertising" or "behavioral advertising."
4. Definition related to a "K-12 purpose" or "school purpose."
5. Other pertinent definitions.

Parties Covered and Regulated

Some state student privacy laws were specifically written to extend legal protections to more categories of students and other parties, and to regulate the use of data by education agencies or private entities. The *Family Educational Rights and Privacy Act (FERPA)*[1] and the *California Student Online Personal Information Protection Act (SOPIPA)*[2] were used to identify which parties are typically covered and regulated in student privacy laws. The following four factors were used to determine each state's grade for the parties covered and regulated:

1. Categories of students covered
2. Private entities or other third parties regulated
3. Categories of other parties covered
4. Education agencies regulated

Grades were based on the total points for this category and assigned an average GPA according to the table in **Figure 1**.

[1] ECFR - Code of Federal Regulations, www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34%3A1.1.1.1.33#se34.1.99_13.

[2] California SB-1177 Privacy: Students. (2013-2014), leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB1177.

Figure 1 - Parties Covered and Regulated | Points Possible = 16

Grade	Point Range	Average GPA	Weight (10%)	Weighted GPA	# States
A+	(15.5)-(16.0)	4.33	*0.10	0.43	0
A	(14.5)-(15.0)	4.00	*0.10	0.40	0
A-	(13.5)-(14.0)	3.67	*0.10	0.37	0
B+	(12.5) -(13.0)	3.33	*0.10	0.33	0
B	(11.0)-(12.0)	3.00	*0.10	0.30	2
B-	(10.0)-(10.5)	2.67	*0.10	0.27	1
C+	(8.5)-(9.5)	2.33	*0.10	0.23	4
C	(6.5)-(8.0)	2.00	*0.10	0.20	9
C-	(5.0)-(6.0)	1.67	*0.10	0.17	8
D+	(3.5)-(4.5)	1.33	*0.10	0.13	7
D	(2.0)-(3.0)	1.00	*0.10	0.10	8
D-	(0.5)-(1.5)	0.67	*0.10	0.07	1
F	0.0	0.00	*0.10	0.00	11

Categories of students covered

Each category of students covered by the law received one point. If no categories were listed, the law received no points. Examples include pre-K, K-12, private school, and post-secondary students. The maximum number of points awarded was capped at four.

Categories of other parties covered

Each category of additional parties covered by the law, not including those referenced above, received one point. If no categories were listed, the law received no points. Examples include teachers, principals, paraprofessionals and other school employees. The maximum number of points awarded was capped at four.

Education agencies regulated

Each agency regulated by a majority of provisions under the law received one point; and each agency regulated by limited provisions of the law received 0.5 points. If no agency was identified, the law received no points. Examples of educational agencies include the state board of education, state department of education, local school districts, public schools, charter schools, and private schools. The maximum number of points awarded was capped at four.

Private entities or third parties regulated

Each private entity or third party regulated by a majority of provisions under the law received one point; and each private entity or third party regulated by limited provisions of the law received 0.5 points. If no entities were indicated, the law received no points. Examples of private entities or third parties include vendors, operators, online service providers, and researchers. The maximum number of points awarded was capped at four.

Transparency

The following four factors were used to determine each state's grade for transparency:

1. Education agency data transparency
2. Executed written agreements
3. Transparency of written agreements
4. Written agreement baseline requirements

Grades were based on the total points for this category and assigned an average GPA according to the table in **Figure 2**.

Figure 2 - Transparency | Points Possible = 16

Grade	Point Range	GPA	Weight (15%)	Weighted GPA	# States
A+	(14.5)-(16.0)	4.33	*0.15	0.65	0
A	(11.5)-(14.0)	4.00	*0.15	0.60	0
A-	(9.5)-(11.0)	3.67	*0.15	0.55	0
B+	(8.5)-(9.0)	3.33	*0.15	0.50	2
B	(7.5)-(8.0)	3.00	*0.15	0.45	1
B-	(6.5)-(7.0)	2.67	*0.15	0.40	1
C+	(5.5)-(6.0)	2.33	*0.15	0.35	4
C	(4.0)-(5.0)	2.00	*0.15	0.30	5
C-	(3.0)-(3.5)	1.67	*0.15	0.25	2
D+	(2.0)-(2.5)	1.33	*0.15	0.20	2
D	(1.0)-(1.5)	1.00	*0.15	0.15	5
D-	(0.5)	0.67	*0.15	0.10	0
F	0.0	0.00	*0.15	0.0	29

For purposes of this section:

- "*Education agency*" or "*education agencies*" may include the state board of education, the state department of education, local districts, and schools.
- "*PSI*" or "*protected student information*" means student data specifically protected by the law.
- "*Private entities*" or "*third parties*" may include vendors, contractors, sub-contractors, operators, and researchers.
- "*Written agreements*" may include a formal, negotiated contract or memorandum of understanding (MOU).

Education agency data transparency

Guidelines established in the U.S. Department of Education's Privacy Technical Assistance Center's *Transparency Best Practices for*

Schools[3] document were used to determine to what extent each state student privacy law required education agencies to identify: a) what protected student information (PSI) they collect, b) the purpose/use of each collection, and c) and how this information is made available to parents and the public. Points were awarded as follows:

- All specific PSI data elements collected must be identified (e.g. student first and last name, address, city, zip, phone, cell, etc.), the purpose/use of each collection must be explained, and the elements/use/purpose must be posted publicly on a website or similar = 4;
- All specific PSI data elements collected must be identified (e.g. student first and last name, address, city, zip, phone, cell, etc.), the purpose/use of only certain collections must be explained, and the elements/use/purpose must be posted publicly on a website or similar = 3;
- Only categories of PSI collected must be identified (e.g. student contact information), the use/purpose of the collections must be explained, and the categories/use/purpose must be posted publicly on a website or similar = 2;
- Only categories of PSI collected must be identified (e.g. student contact information), the use/purpose of the collections must be explained, and the categories/use/purpose are available upon request only = 1;
- No requirements are specified = 0 or N/A.

Executed written agreements

Written agreements provide clarity and hold any party to the contract accountable. If a law required education agencies to execute a written agreement before sharing PSI with any third party, it received four points. When written agreements were required with only a limited set of third parties, the law received two points. If no written agreements were required, no points were awarded.

Transparency of written agreements

Making agreements available to the public is of critical importance so that parents may evaluate their contents for adequate data privacy and security. The U.S. Department of Education's Privacy Technical Assistance Center's *Transparency Best Practices for Schools*[4] and the Federal Trade Commission's

[3] Transparency Best Practices for Schools and Districts, Privacy Technical Assistance Center (PTAC), U.S. Department of Education, studentprivacy.ed.gov/sites/default/files/resource_document/file/LEA%20Transparency%20Best%20Practices%20final.pdf.

[4] Ibid.

Complying with COPPA: Frequently Asked Questions[5] guidance for the *Children's Online Privacy Protection Act ("COPPA Rule")*[6] were consulted to establish reasonable metrics for transparency. Points were awarded based on the extent to which the agreements between education agencies and third parties are made available to the public, as follows:

- Written notice must be provided to parents advising them of the existence of written agreements, and agreements must be posted prominently on a public website or in a similar location = 4;
- Written notice must be provided to parents advising them of the existence of written agreements, but public posting is not required = 3;
- Written agreements must be posted prominently on a public website or similar location, but parent notification is not required = 2;
- Written agreements are made available only upon request = 1;
- No requirements for parental notice or public posting of written agreements = 0 or N/A.

Written agreement baseline requirements

The U.S. Department of Education's documents *Written Agreement Checklist*[7] and the *Family Educational Rights and Privacy Act Guidance for Reasonable Methods and Written Agreements*[8] as well as the Fordham Center on Law and Information Policy's report *Privacy and Cloud Computing in Public Schools*[9] were consulted to determine a point scale for baseline requirements in written documents. Points were awarded based on the extent to which executed written agreements between education agencies and third parties include the following information: the PSI collected or shared; the purpose/use of PSI; the process by which parents can access and correct PSI; data retention and destruction procedures; and prohibitions against re-disclosures or subsequent disclosures of PSI information to others (e.g. subcontractors).

---

[5] Complying with COPPA: Frequently Asked Questions. Federal Trade Commission, 25 June 2018, www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[6] ECFR - Code of Federal Regulations, www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5.

[7] Written Agreement Checklist, Privacy Technical Assistance Center (PTAC), U.S. Department of Education, studentprivacy.ed.gov/sites/default/files/resource_document/file/Written_Agreement_Checklist.pdf.

[8] The Family Educational Rights and Privacy Act Guidance for Reasonable Methods and Written Agreements, Privacy Technical Assistance Center (PTAC), U.S. Department of Education, studentprivacy.ed.gov/sites/default/files/resource_document/file/Guidance_for_Reasonable_Methods%20final_0.pdf.

[9] Reidenberg, Joel. "Privacy and Cloud Computing in Public Schools." FLASH: The Fordham Law Archive of Scholarship and History, ir.lawnet.fordham.edu/clip/2/.

Points were awarded as follows:

- Written agreements must include all the requirements enumerated = 4;
- Written agreements must include 3-4 of the requirements enumerated = 3;
- Written agreements must include 1-2 of the requirements enumerated = 2;
- Written agreements do not include the requirements enumerated but must include other requirements = 1;
- No specific requirements are enumerated = 0 or N/A.

Parental and Student Data Rights

States received grades based on the extent to which they afforded parents and students basic data rights. Grades were based on the following seven factors:

1. Parents' right to access, correct and delete protected student information, and to prohibit further collection
2. Prohibitions against the collection of sensitive student information by schools, and its disclosure to third parties
3. Prohibitions against the state's collection of sensitive student information
4. Prohibitions against the disclosure of protected student information to the federal government by schools or the state
5. Prohibitions against the development of student profiles by private entities
6. Prohibitions against the disclosure of protected student information by private entities
7. Prohibitions against the re-disclosure of protected student information by private entities

Grades were based on the total points for this category and assigned an average GPA according to the table in **Figure 3**.

Figure 3 - Parental and Student Data Rights | Points Possible = 26

Grade	Point Range	GPA	Weight (20%)	Weighted GPA	# States
A+	(23.5)-(26.0)	4.33	*0.20	0.87	0
A	(20.5)-(23.0)	4.00	*0.20	0.80	0
A-	(17.5)-(20.0)	3.67	*0.20	0.73	0
B+	(15.0)-(17.0)	3.33	*0.20	0.67	2
B	(12.0)-(14.5)	3.00	*0.20	0.60	1
B-	(9.5)-(11.5)	2.67	*0.20	0.53	3
C+	(8.0)-(9.0)	2.33	*0.20	0.47	2
C	(5.5)-(7.5)	2.00	*0.20	0.40	9
C-	(4.0)-(5.0)	1.67	*0.20	0.33	8
D+	(3.0)-(3.5)	1.33	*0.20	0.27	5
D	(1.5)-(2.5)	1.00	*0.20	0.20	3
D-	(0.5)-(1.0)	0.67	*0.20	0.13	0
F	0.0	0.0	*0.20	0.00	18

For purposes of this section:

- "*Education agency*" or "*education agencies*" may include the state board of education, the state department of education, local districts, and schools.
- "*PSI"* or "*protected student information"* means student data specifically protected by the law.
- "*Private entities*" or "*third parties*" may include vendors, contractors, subcontractors, operators, and researchers.
- "*Written agreements*" may include a formal, negotiated contract or memorandum of understanding (MOU).

Parents' right to access, correct and delete protected student information, and to prohibit further collection

The *Family Educational Rights and Privacy Act (FERPA)*[10] and the *Children's Online Privacy Protection Act (COPPA)*[11] provide a low threshold of rights for parents and eligible students to access, correct, and in limited cases, delete and prohibit the future collection of student data. Using FERPA and COPPA as sources, a point scale was applied to each state law according to the extent that parents are allowed to access and correct PSI received or collected by third parties, delete the information if it is in error or is "nonessential to the student's education record," and opt-out of further collection. Points were awarded as follows:

[10] ECFR - Code of Federal Regulations, www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34%3A1.1.1.1.33#_top.

[11] Children's Online Privacy Protection Rule ('COPPA'). Federal Trade Commission, 5 Apr. 2018, www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

- Parents are allowed to access, correct, and delete erroneous/nonessential PSI, and opt-out of further collection held by any private entity or third party = 4;
- Parents are allowed to access, correct, and delete erroneous/nonessential PSI but not opt-out of further collection held by any private entity or third party = 3;
- Parents are allowed to access, correct, and delete erroneous/nonessential PSI, but not opt-out of further collection, held by a limited set of private entities or third parties = 2;
- Parents are allowed only to access and correct PSI held by a limited set of private entities or third parties = 1;
- No express rights are given to parents to access, correct, delete and opt-out of further collected of PSI = 0 or N/A.

Prohibitions against the collection of sensitive student information by schools, and its disclosure to third parties

Many parents believe some student information is so sensitive that it should never be collected by schools; or if it is collected, it should never be disclosed to non-governmental private entities without parental consent. Examples of such sensitive student information may include Social Security numbers and biometric data. Non-governmental private entities include vendors, contractors, subcontractors, operators, and community organizations. Points were awarded as follows:

- Certain sensitive information cannot be collected at all = 4;
- Certain sensitive student information cannot be collected without parental consent = 3;
- Certain sensitive student information cannot be disclosed to private entities or other third parties = 2;
- Certain sensitive student information cannot be disclosed to private entities or other third parties without parental consent = 1;
- There are no restrictions on collections or disclosures of sensitive student information = 0 or N/A.

Prohibitions against the collection of sensitive student information by the state

Parents believe strongly that certain sensitive student information should be available only to the school and its employees directly serving the child. Laws preventing the state department of education or other related state agencies from collecting sensitive student information directly from students or from schools or districts received one point for each data element prohibited. If no elements are listed, the law was awarded no points. Examples of sensitive student information include health, disability, and disciplinary information. The maximum number of points awarded was capped at 4.

Prohibitions against the disclosure of protected student information to the federal government by schools or the state

Not unlike prohibitions on sensitive student information data collections by the state, parents wish to prevent the federal government and their assignees, including researchers, from receiving this and other student information. In cases where the state department of education and/or school districts are prohibited from disclosing PSI to the federal government or its assignees, the law received two points. When disclosure is allowed only with parental consent, the law received one point. Laws with no prohibitions received no points.

Prohibitions against the development of student profiles by third parties

Data collected through technology services are often used to create individual student profiles. Profiles developed for "educational purposes" may be used to make instructional decisions about a student based on her interests, abilities and predicted performance. Profiles created for "non-educational purposes" are often used to market or advertise to a student or his parents. Both uses are a threat to a student's privacy.

California's *Student Online Private Information Protection Act*,[12] and the *Student Privacy Pledge*[13] developed by the Future of Privacy Forum and the Software & Information Industry Association were the first large-scale attempts to address this relatively new phenomenon, but in our view fell short to satisfy parental concerns about the potential misuse of student data.

We evaluated each state law by the extent to which third parties receiving or collecting PSI are permitted to develop student profiles. Points were awarded based on the following scale:

- Third parties are prohibited from developing student profiles for any purpose = 4;
- Third parties are prohibited from developing student profiles for non-educational purposes, and must obtain parental consent to develop student profiles for educational purposes = 3;
- Third parties must obtain parental consent to develop student profiles for educational purposes = 2;
- Third parties are limited to developing student profiles for educational purposes only, but can do so without parental consent = 1;

[12] California SB-1177 Privacy: Students. (2013-2014), leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB1177.

[13] Privacy Pledge – Pledge to Parents & Students. Future of Privacy Forum (FPF) and The Software Information Industry Association (SIIA), studentprivacypledge.org/.

Third parties are permitted to develop student profiles for any purpose authorized by the school or district, or for non-educational purposes with the consent of parents, students, or other authorized individuals = 0 or N/A.

Prohibitions against the disclosure of protected student information by private entities

The risk of breaches, hacks, and other unauthorized use of PSI increases with the number of data disclosures. Therefore, limiting disclosures is one way to protect the privacy of students. The point scale used to measure the extent to which private entities collecting PSI directly from students or from schools are permitted to disclose the information to other third parties, including sub-contractors and other service providers, for educational and non-educational purposes is as follows:

- Private entities are prohibited from disclosing PSI to any other third party for any reason = 4;
- Private entities are prohibited from disclosing PSI to any other third party for non-educational purposes, and must obtain parental consent to disclose PSI to any third party for educational purposes = 3;
- Private entities are permitted to disclose PSI to third parties for educational purposes without parental consent, and/or for non-educational purposes with parental consent = 2;
- Private entities are permitted to disclose PSI to a limited number of other third parties for various purposes with or without parental consent = 1;
- There are no limits on the potential redisclosures by private entities of PSI, or the law does not specifically address this issue = 0 or N/A.

Prohibitions against the redisclosure or subsequent disclosures of protected student information by private entities

Redisclosure or subsequent disclosures of PSI by one private entity to another presents an additional privacy threat. The *California Student Online Personal Information Protection Act (SOPIPA)*[14] was used as a source since it was the first state privacy law to curb redisclosures by third parties. The point scale to measure the extent to which third parties, including email service providers, receiving PSI from third parties including vendors, operators, and researchers, are permitted to redisclose the information to other third parties, including cloud storage providers, is as follows:

- Third parties are prohibited from redisclosing PSI to any other third party = 4;
- Third parties are prohibited from redisclosing PSI to any other third party without parental consent = 3;

[14] California SB-1177 Privacy: Students. (2013-2014), leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB1177.

- Third parties are permitted to redisclose PSI to specifically identified third parties for educational purposes only with parental consent = 2;
- Third parties are permitted to redisclose PSI to other third parties subject to a contract or in accordance with provisions of the law = 1;
- Redisclosure is not specifically addressed = 0 or N/A.

Limitations on Commercial Use of Data

States received grades based on the extent to which they prohibited the commercialization of protected student information. Grades were based on the following five factors:

1. Prohibitions against selling protected student information by education agencies
2. Prohibitions against selling protected student information by third parties
3. Prohibitions against using protected student information for targeted or behavioral advertising purposes by third parties
4. Prohibitions against using protected student information for commercial purposes by third parties
5. Prohibitions against using de-identified or aggregate student information for commercial purposes by third parties

Grades were based on the total points for this category and assigned an average GPA according to the table in **Figure 4**.

Figure 4 - Limitation on Commercial Use of Data | Points Possible = 14

Grade	Point Range	GPA	Weight (20%)	Weighted GPA	# States
A+	(13.0)-(14.0)	4.33	*0.20	0.87	0
A	(11.5)-(12.5)	4.00	*0.20	0.80	0
A-	(10.0)-(11.0)	3.67	*0.20	0.73	1
B+	(8.5)-(9.5)	3.33	*0.20	0.67	0
B	(6.5)-(8.0)	3.00	*0.20	0.60	1
B-	(5.0)-(6.0)	2.67	*0.20	0.53	4
C+	(4.5)	2.33	*0.20	0.47	0
C	(3.0)-(4.0)	2.00	*0.20	0.40	19
C-	(2.5)	1.67	*0.20	0.33	0
D+	(2.0)	1.33	*0.20	0.27	3
D	(1.0)-(1.5)	1.00	*0.20	0.20	1
D-	(0.5)	0.67	*0.20	0.13	0
F	0.0	0.00	*0.20	0.00	20
F	(-0.5)	-0.67	*0.20	-0.13	0
F	(-1.0)-(-1.5)	-1.00	*0.20	-0.20	1
F	(-2.0)	-1.33	*0.20	-0.27	0
F	(-2.5)	-1.67	*0.20	-0.33	0
F	(-4.0)-(-3.0)	-2.00	*0.20	-0.40	1

For purposes of this section:

- "*Education agency*" or "*education agencies*" may include the state board of education, the state department of education, local districts, and schools.
- "*PSI"* or "*protected student information"* means student data specifically protected by the law.
- "*Private entities*" or "*third parties*" may include vendors, operators, and researchers.
- "*Written agreements*" may include a formal, negotiated contract or legally enforceable memorandum of understanding (MOU).

Prohibitions against selling protected student information by education agencies

Schools should not be in the business of selling student data for any purpose. Laws that prohibit the sale of PSI by education agencies, including the state department of education, local districts, and schools, in all circumstances received two points. If the issue is not addressed, the law received 0 or N/A point. When the sale is allowable under specified circumstances, such as for contracted services, we subtracted two points.

Prohibitions against selling protected student information by third parties

To protect privacy, restrictions must be placed on private entities from selling PSI. California's *Student Online Private Information Protection Act*,[15] and the *Student Privacy Pledge*[16] introduced by the Future of Privacy Forum and the Software & Information Industry Association were introduced to try to limit this practice. Points were awarded based on the extent to which private entities are prohibited from selling PSI. Where sale of student data is allowed outside of mergers, acquisitions, asset sales, or bankruptcies, points were subtracted. Points were assigned based on the following:

- Sale of PSI by private entities is banned in all circumstances = 4;
- Sale of PSI by private entities is banned in certain circumstances, including for contracted services, or by specific regulated parties, including cloud service providers = 3;
- Sale of PSI by private entities is allowed in mergers, acquisitions, asset sales, or bankruptcies; however, the purchasing party must comply with any privacy protections established by the original party or under the law = 2;
- Sale of PSI by private entities is allowed in mergers, acquisitions, asset sales, or bankruptcies; however, the

[15] Ibid.

[16] Privacy Pledge – Pledge to Parents & Students. Future of Privacy Forum (FPF) and The Software Information Industry Association (SIIA), studentprivacypledge.org/.

purchasing party is not obligated to comply with any privacy protections established by the original party or under the law = 1;
- Sale of PSI is not addressed = 0 or N/A;
- Sale of PSI is allowed outside of mergers, acquisitions, asset sales, or bankruptcies = -2.

Prohibitions against using protected student information for targeted or behavioral advertising purposes by third parties

Students using technology services assigned by schools should not have their personal information used for advertising purposes. While the Federal Trade Commission's COPPA Rule[17] established baseline standards this area, the rule is inadequate as it only protects the data of children under the age of 13. Using COPPA's language as a reference, points were awarded based on the extent to which private entities are prohibited from using PSI for marketing purposes, including for targeted advertising for all students when using online products or services assigned by their schools. Points were assigned based on the following:

- Targeted advertising to students by private entities using PSI is banned in all cases = 4;
- Targeted advertising to students by private entities using PSI is banned in limited circumstances, including as specified in contracts with operators or service providers = 3;
- Targeted advertising to students by private entities using PSI is allowed under a single exception, including based on a student's one-time visit to a website = 2;
- Targeted advertising to students by private entities using PSI is allowed under two or more exceptions, including based on a student's one-time visit to a website, and when a student is performing a search query = 1.
- Not addressed = 0 or N/A.

Prohibitions against using protected student information for commercial purposes by third parties

The use of personal student information by education technology companies, including vendors and operators, should be limited to activities that directly benefit the student. Other uses of this information for non-educational or commercial purposes, including to develop or improve new products or services, should be strictly prohibited. Laws that prohibit all third parties from using PSI for these purposes received two points. If third parties are permitted to use PSI or "information" (an undefined term used in some SOPIPA-like laws) to maintain, develop, support, or improve their products

[17] ECFR - Code of Federal Regulations, www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5.

and services, or the issue is not addressed, the law received no points.

Prohibitions against using de-identified or aggregate student information for non-educational purposes by third parties

De-identifying or stripping data of information such as name and date of birth or aggregating large quantities of data are practices intended to protect the identity of individuals. The U.S. Department of Education's guidance titled, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices,* claims that properly "de-identified" student data can be disclosed and used for various purposes without parental consent, including to develop or improve products and services.[18]

Since rigorous guidelines do not yet exist to ensure that even de-identified education data cannot be re-identified, laws prohibiting third parties from using de-identified or aggregate student information for non-educational purposes were awarded two points. If third parties were expressly permitted to use de-identified or aggregate student information for non-educational purposes, or the issue is unaddressed, the law was awarded no points.

Data Security Requirements

States received grades based on the extent to which they require education agencies or private entities to secure the data from breaches or other unauthorized disclosures. Grades were based on the following three factors:

1. Required implementation of a basic data security program by education agencies
2. Required implementation of a basic data security program by private entities
3. Breach notification policies to affected families

Grades were based on the total points for this category and assigned an average GPA according to the table in **Figure 5**.

[18] Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, Privacy Technical Assistance Center (PTAC), U.S. Department of Education, https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

Figure 5 - Data Security Requirements | Points Possible = 12

Grade	Point Range	GPA	Weight (15%)	Weighted GPA	# States
A+	(11.5)-(12.0)	4.33	*0.15	0.65	0
A	(9.5)-(11.0)	4.00	*0.15	0.60	0
A-	(8.5)-(9.0)	3.67	*0.15	0.55	0
B+	(8.0)	3.33	*0.15	0.50	1
B	(7.0)-(7.5)	3.00	*0.15	0.45	0
B-	(6.5)	2.67	*0.15	0.40	3
C+	(5.5)-(6.0)	2.33	*0.15	0.35	5
C	(4.5)-(5.0)	2.00	*0.15	0.30	5
C-	(3.5)-(4.0)	1.67	*0.15	0.25	6
D+	(2.5)-(3.0)	1.33	*0.15	0.20	0
D	(1.5)-(2.0)	1.00	*0.15	0.15	13
D-	(0.5)-(1.0)	0.67	*0.15	0.10	2
F	0.0	0.00	*0.15	0.0	16

For purposes of this section:

- "*Education agency*" or "*education agencies*" may include the state board of education, the state department of education, local districts, and schools.
- "*PSI"* or "*protected student information"* means student data specifically protected by law.
- "*Private entities*" may include vendors, operators, contractors, subcontractors and researchers.
- "*Written agreements*" may include a formal, negotiated contract or memorandum of understanding (MOU).

Required implementation of a data security program by education agencies

The U.S. Department of Education's Privacy Technical Assistance Center provides data security guidance to education agencies on how to protect the student information they collect and maintain. As outlined in the Department's *Data Security Checklist*[19] and *Data Governance Checklist*[20] documents, best practices for data security programs include, but are not limited to, authentication, access controls, physical safety of hardware, training of personnel, and audit and compliance monitoring.

All of the above elements in the checklist are critical to ensure proper data security protections. We created a point system to

[19] Data Security Checklist, Privacy Technical Assistance Center (PTAC), U.S. Department of Education, studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Security%20Checklist_0.pdf.

[20] Data Governance Checklist, Privacy Technical Assistance Center (PTAC), U.S. Department of Education, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Governance%20Checklist_0.pdf.

measure the number of components required by state law. Points were awarded as follows:

- Education agencies are required to implement a security program with five or more components from the checklist = 4;
- Education agencies are required to implement a security program with three to four components = 3;
- Education agencies are required to implement a security program with one to two components = 2;
- Education agencies are required to implement unspecified "industry standards" for a security program = 1;
- Education agencies are required to "develop" but not implement any security program = 0 or N/A.

Required implementation of a data security program by third parties

Just as education agencies must implement a basic security program to protect student information, any authorized private entity collecting or receiving this information must also be required to implement basic security protections. Using the same source document and scale as above, points were awarded as follows:

- Private entities collecting or receiving PSI are required to implement a security program with five or more components = 4;
- Private entities collecting or receiving PSI are required to implement a security program with three to four components = 3;
- Private entities collecting or receiving PSI are required to implement a security program with one to two components = 2;
- Private entities collecting or receiving PSI, and any subsequent third parties collecting or receiving PSI are required to implement unspecified "industry standards" or "reasonable standards" for security = 1.5;
- Private entities collecting or receiving PSI are required to implement unspecified "industry standards" or
- "reasonable standards" for security = 1;
- No mention of requirements = 0 or N/A.

Breach notification

The U.S. Department of Education's Privacy Technical Assistance Center provides guidance to education agencies responding to data breaches with the document entitled *Data Breach Response Checklist*.[21] Using this guidance as a framework, the following point system was established to measure the extent to which education agencies or private entities collecting or received PSI must notify parents of data breaches:

- Education agencies or private entities are required to notify parents of all suspected and verified breaches of PSI within 10 days of an incident = 4;
- Education agencies or private entities are required to notify parents of all suspected and verified breaches of PSI within a "reasonable" timeframe = 3;
- Education agencies or private entities are required to notify parents of all verified breaches of PSI within 10 days of an incident = 2;
- Education agencies or private entities are required to notify parents of all verified breaches of PSI within a "reasonable" or unspecified timeframe, or more than 10 days after the incident = 1;
- Education agencies or private entities must address unauthorized access of PSI, but parental notification is not required or no other specifics are given = 0.5;
- No mention of breach notification = 0 or N/A.

Oversight, Enforcement, and Penalties for Violations

States received grades based on the extent to which they specified enforcement mechanisms in the law and cited fines or penalties. Grades were based on the following six factors:

1. Regulating authority is identified
2. Enforcement process is identified
3. Fines or penalties for violations are enumerated
4. Chief Privacy Officer (CPO) or similar is mandated
5. Citizen stakeholder oversight board or similar is mandated
6. Private right of action exists, allowing students whose information is breached or improperly disclosed to sue the responsible party

Grades were based on the total points for this category and assigned an average GPA according to the table in **Figure 6**.

[21] Data Breach Response Checklist, Privacy Technical Assistance Center (PTAC). U.S. Department of Education, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf.

Figure 6 - Oversight, Enforcement, and Penalties for Violation | Points Possible = 12

Grade	Point Range	GPA	Weight (15%)	Weighted GPA	# States
A+	(12.0)	4.33	*0.15	0.65	0
A	(11.0)-(11.5)	4.00	*0.15	0.60	0
A-	(10.5)	3.67	*0.15	0.55	0
B+	(10.0)	3.33	*0.15	0.50	1
B	(8.5)-(9.5)	3.00	*0.15	0.45	0
B-	(8.0)	2.67	*0.15	0.40	1
C+	(7.0)-(7.5)	2.33	*0.15	0.35	0
C	(5.0)-(6.5)	2.00	*0.15	0.30	5
C-	(4.0)-(4.5)	1.67	*0.15	0.25	8
D+	(3.0)-(3.5)	1.33	*0.15	0.20	0
D	(1.5)-(2.5)	1.00	*0.15	0.15	8
D-	(0.5)-(1.0)	0.67	*0.15	0.10	0
F	0.0	0.00	*0.15	0.0	28

Regulating authority is identified

Laws identifying a regulating authority, other than the state department of education, received two points. If no regulating authority was specified, the law received no points.

Enforcement process is identified

Laws describing an enforcement process received 2 points. If an enforcement process was omitted, the law was awarded no points.

Fines or penalties for violations are enumerated

Laws that enumerated fines or penalties for violations, including breaches, were awarded two points. Laws omitting fines or penalties received no points.

Chief Privacy Officer (CPO) or similar position is mandated

If a law mandated the creation of a state Chief Privacy Officer (CPO) or similar position, it received two points. If no CPO or similar position was mandated, the law received no points.

Citizen stakeholder board or similar committee is mandated

Laws mandating the creation of a citizen or stakeholder student data oversight board or committee were awarded two points. If no board or committee was mandated, the law received no points.

Private right of action

Each law that enumerated a private right of action received two points; laws with no private right of action received no points.

Other Provisions

Additional provisions in state laws, either positive or negative in their impact on student privacy

As explained in the Components and Categories to Calculate State Grades section, each protective measure contained in a state law that did not fit into any of our categories received +0.5 points; each provision that weakened student data privacy was assigned -0.5 points. The maximum and minimum number of points awarded were capped at +/-4.

Grades were based on the total points for this category and assigned an average GPA according to the table in **Figure 7**.

Figure 7 - Other Provisions | Points Possible +/-4

Grade	Point Range	GPA	Weight (5%)	Weighted GPA	# States
A	(4.0)	4.00	*0.05	0.20	0
B+	(3.5)	3.33	*0.05	0.17	1
B	(3.0)	3.00	*0.05	0.15	0
C+	(2.5)	2.33	*0.05	0.12	2
C	(2.0)	2.00	*0.05	0.10	1
D+	(1.5)	1.33	*0.05	0.07	4
D	(1.0)	1.00	*0.05	0.05	4
D-	(0.5)	0.67	*0.05	0.03	6
F	0.0	0.00	*0.05	0.0	15
F	(-0.5)	-0.67	*0.05	-0.03	4
F	(-1.0)	-1.00	*0.05	-0.05	5
F	(-1.5)	-1.33	*0.05	-0.07	5
F	(-2.0)	-2.00	*0.05	-0.10	4
F	(-2.5)	-2.33	*0.05	-0.12	0
F	(-3.0)	-3.00	*0.05	-0.15	0
F	(-3.5)	-3.33	*0.05	-0.17	0
F	(-4.0)	-4.00	*0.05	-0.20	0

PARENT COALITION FOR
STUDENT PRIVACY

www.studentprivacymatters.org

THE NETWORK FOR
PUBLIC EDUCATION

www.networkforpubliceducation.org