



AMC 2025

Session 6

Children's Data Privacy

Presented by:

Ryan R. Johnson, Savvas Learning Company, Phoenix, AZ

About the Presenter...

Ryan R. Johnson is a certified SME in data privacy and cybersecurity, a seasoned public speaker and author with over 25 years of experience spanning business and technology. He currently serves as Chief Privacy Officer, Vice President, and Associate General Counsel at Savvas Learning Company and is a board member at Lake Trust Credit Union. Ryan's passion for education and privacy is reflected in his prior role as a law professor, where he specialized in teaching courses on data privacy. He continues to champion responsible data practices that protect children while advancing innovation in education technology. His commitment to transparency, economic empowerment, and inclusivity reflects both his professional achievements and dedication to ongoing personal growth.

Ryan Johnson, FIP
Chief Privacy Officer, VP,
Associate General Counsel
Savvas Learning Company LLC

Children's Data Privacy: Navigating Legal and Regulatory Landscapes

Disclaimer: This material is for informational and educational purposes only and does not constitute legal advice. Laws and regulations in this area are complex and may change. The views expressed herein are those of the presenter in a personal capacity and do not represent Savvas Learning Company.

Introduction to Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) and the Federal Trade Commission's (FTC) implementing rule (COPPA Rule) are designed to provide enhanced privacy protections for children under 13 online.

Applicability and Scope

An operator is subject to COPPA if their site or service collects personal information from or about users and is directed to children under 13. This broad applicability includes a range of network-connected products and services such as mobile apps, network-connected video games, and social media sites. Platform operators with actual knowledge of child-directed content are also subject to COPPA.¹

Defining "Personal Information" and Collection Methods

"Personal information" under COPPA includes information collected from a child online that identifies the child or their parents, persistent identifiers, and biometric and geolocation data. Collection methods encompass both requesting, prompting, or encouraging users to submit information and passive tracking through technologies like cookies and other identifiers.²

¹ *Children's Online Privacy Protection Act (COPPA) Compliance Checklist | Practical Law*, [https://1.next.westlaw.com/Document/I5f5954321c8a11e38578f7ccc38dcbee/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd910000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI5f5954321c8a11e38578f7ccc38dcbee%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=2&sessionScopeId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=\(sc.Search\)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD](https://1.next.westlaw.com/Document/I5f5954321c8a11e38578f7ccc38dcbee/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd910000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI5f5954321c8a11e38578f7ccc38dcbee%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=2&sessionScopeId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD) (last visited May 9, 2025).

² *Children's Online Privacy: COPPA Compliance | Practical Law*, [https://1.next.westlaw.com/Document/I5f7b8998bc3f11e398db8b09b4f043e0/View/FullText.html?originationContext=document&vr=3.0&rs=cb1t1.0&transitionType=DocumentItem&contextData=\(sc.Search\)+&__lrTS=20250530193312521](https://1.next.westlaw.com/Document/I5f7b8998bc3f11e398db8b09b4f043e0/View/FullText.html?originationContext=document&vr=3.0&rs=cb1t1.0&transitionType=DocumentItem&contextData=(sc.Search)+&__lrTS=20250530193312521) (last visited May 30, 2025).

Core COPPA Requirements and Compliance Basics

A fundamental principle underlying COPPA is the recognition that children may not fully understand the consequences of sharing their personal information and thus lack the legal capacity to consent. Operators subject to COPPA must comply with requirements related to parental notice and obtaining verifiable parental consent before collecting, using, or disclosing personal information from children.³

Key compliance requirements include:

- **Required Privacy Policy Disclosures:** The privacy policy must clearly describe:
 - The data elements collected from children and how they are collected (e.g., directly, passive tracking).
 - Whether children can make personal information publicly available.
 - How the company may use children's information.
 - Practices for disclosing information, the types of information disclosed, and how third parties may use it.
 - Details on third-party sharing, including who the information is shared with, what categories of data are shared, and data retention practices.
 - Procedures for parents to exercise their rights regarding their children's information.⁴
- **Privacy Policy Placement:** Links to the privacy policy must be clear and prominently labeled on the home/landing page and near all data collection points. For mobile apps, visibility in the app store and within the app with distinct formatting is required.
- **Parental Access and Control:** Parents are granted rights to access and control their children's information.⁵

COPPA Updates (2025)

The FTC have implemented key updates to COPPA for a more robust approach to children's data privacy:

³ *Id.*

⁴ Children's Online Privacy Protection Act (COPPA) Compliance Checklist | Practical Law, *supra* note 1.

⁵ Children's Online Privacy: COPPA Compliance | Practical Law, *supra* note 2.

- **Expanded Age Coverage:** Protections now extend to teens aged 13–16, allowing them to consent or exercise rights in certain cases.
- **Broader Personal Information Definition:** The definition of personal information has been expanded to include persistent identifiers, photos, videos, audio, geolocation data, and biometric data.
- **Updated "Actual Knowledge":** The concept of "actual knowledge" of child-directed content may now include knowledge implied from objective circumstances.
- **"Directed to Children" Test:** The determination of whether a site or service is "directed to children" is now based on the totality of circumstances, including audience data and intent.
- **Targeted Ads Ban:** The use of children's or teens' data for targeted advertising is now prohibited.
- **Data Minimization:** Collection of personal information is limited to what is contextually necessary.
- **Notice & Consent:** Direct notice and new consent are required for material changes to data practices. Additionally, foreign data transfers without notice are banned.
- **Enhanced Rights:** New rights include access, correction, deletion, and transparency regarding data source and purpose.
- **Retention Limits:** Data must not be kept longer than necessary for its intended purpose.
- **Deletion Requirements:** Operators must delete data when it is no longer needed or upon parent request. Service cannot be denied solely due to a deletion request, with some exceptions.⁶

⁶ *US Children's Privacy Legislation Tracker | Practical Law*,

[https://1.next.westlaw.com/Document/I23de7479aee411ee8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9feb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI23de7479aee411ee8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=9&sessionScopeId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=\(sc.Search\)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD](https://1.next.westlaw.com/Document/I23de7479aee411ee8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9feb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI23de7479aee411ee8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=9&sessionScopeId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD) (last visited May 9, 2025).

COPPA Compliance Measures & Safe Harbor

Compliance and security measures under COPPA have also seen updates:

- **Notice & Consent Alternative:** Consent is not required if a site is not child-directed and no personal information is knowingly collected.
- **Data Protection:** Operators must maintain reasonable safeguards, including a written information security program (WISP).
- **Third-Party Disclosures:** Before sharing children's data with third parties, operators must vet them and obtain written assurances. Contracts with third-party partners should confirm if they collect personal information, assess their practices, and limit data collection via contract.
- **Data Retention:** A written data retention policy should be included in the privacy notice. Data must be deleted when no longer needed or upon parental request, using secure disposal methods.
- **Ongoing Compliance:** Regular review of policies, consent methods, and vendor practices is crucial. Auditing data handling and parental access compliance should also be conducted regularly.
- **Safe Harbor Option:** Operators can join an FTC-approved program as an alternative to direct enforcement. Examples of such programs include CARU, ESRB, TRUSTe, Privo, iKeepSafe, and kidSAFE. As of 2025, the FTC may begin publicly posting certain Safe Harbor operator submissions.⁷

Student Data Privacy Regulation - Federal Laws

K12 data requires stronger protections than adult data, necessitating EdTech providers to follow federal and state laws and industry standards.

Family Educational Rights and Privacy Act (FERPA)

FERPA governs the privacy of student education records and applies to schools and third-party providers handling student data. It limits access and disclosure of student data, usually requiring written consent for sharing Personally Identifiable Information (PII). The Department of Education (DOE) offers guidance for service providers.

⁷ *Id.*

Protection of Pupil Rights Amendment (PPRA)

PPRA covers surveys, marketing, and notice requirements, applying to third-party providers. Annual and event-based notices must be provided to parents, and providers must inform schools of relevant activities.

COPPA's Role in Student Data Privacy

COPPA also applies to online data collection from children under 13, requiring privacy notices, parental consent, and options for access and control.⁸

FERPA vs. COPPA - Key Differences & Overlap

Understanding the distinctions and intersections of FERPA and COPPA is critical for legal practitioners in the education technology space.

Purpose

- **FERPA:** Primarily protects the privacy of student education records.
- **COPPA:** Specifically protects PII collected online from children under 13.

Applicability

- **FERPA:** Applies to schools, school districts, and third-party service providers acting on their behalf.
- **COPPA:** Applies to website and app operators directed to children under 13 or with actual knowledge of such users.

Consent Required

- **FERPA:** Requires written parental consent for disclosure of PII in education records.
- **COPPA:** Requires verifiable parental consent before collecting personal information from children under 13.

⁸ *Student Privacy: Education Service Provider Requirements | Practical Law*, [https://1.next.westlaw.com/Document/Iaa4293eea8ee11e598dc8b09b4f043e0/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DIaa4293eea8ee11e598dc8b09b4f043e0%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=6&sessionScopeId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=\(sc.Search\)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD#co_anchor_a000065](https://1.next.westlaw.com/Document/Iaa4293eea8ee11e598dc8b09b4f043e0/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DIaa4293eea8ee11e598dc8b09b4f043e0%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=6&sessionScopeId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD#co_anchor_a000065) (last visited May 9, 2025).

When Consent Is Not Required

- **FERPA:** Schools can share data with third-party providers under a written agreement for educational purposes.
- **COPPA:** No consent is required if a school authorizes the use of an edtech tool for educational purposes (with the school acting as an intermediary).⁹

Common Misunderstanding

A common misunderstanding is that schools authorizing edtech tools always need to collect separate COPPA consent. This is not the case if the authorization is done under FERPA-compliant agreements.

Student Data Privacy - FTC Guidance & State Laws

FTC EdTech Guidance

The FTC offers specific guidance for EdTech companies:

- Limit data collection to what is necessary for the activity.
- Data collected via schools must not be used for marketing.
- Do not retain children's data longer than needed.
- Implement reasonable security measures.
- The FTC will closely monitor COPPA compliance in EdTech.¹⁰

State Student Privacy Laws

State student privacy laws are often stricter than federal law and vary significantly by state. Common focus areas include:

- **Contracts:** Must include parent rights, data security, and disposal terms.
- **Security:** Require minimum standards, audits, and breach protocols.
- **Marketing:** Restrict the use of student data for commercial purposes.
- **California Laws:** The Student Online Personal Information Protection Act (SOPIPA) bans targeted ads, requires security, and mandates deletion upon

⁹ *Id.*

¹⁰ *Id.*

school request. The California Age-Appropriate Design Code applies to services likely used by those under 18.¹¹

Enforcement Snapshot - Real-World Examples

The FTC is actively enforcing children's privacy laws, and penalties for non-compliance are significant.

- **YouTube/Google (2019):** Fined \$170M by the FTC and New York Attorney General for COPPA violations, specifically for tracking children's viewing history for ad targeting without parental consent.
- **Epic Games (2022):** Fined \$275M for violating children's privacy, including retention of children's data without consent.
- **Edmodo (2023):** Reached a \$6M settlement for collecting student data without proper parental consent and retaining it beyond what was needed.

Key Takeaway: Contracts and policies must reflect compliant data collection, use, and deletion practices.¹²

Student Data Privacy – Wisconsin

Wisconsin has specific statutes governing student data privacy.

Key Statutes

Wisconsin Statutes § 118.125 (Pupil Records) and § 115.297 cover student data privacy.

Covered Entities and Students

These statutes cover public K–12 schools and districts (with no provisions for third-party vendors), as well as K–12 students under § 118.125 and university students under § 115.297.

Pupil Records and Student Data Definitions

"Pupil Records" refer to records related to individual students maintained by schools, excluding personal notes, psychological treatment records, and law enforcement records. "Student Data" is defined as "education records" per 34 C.F.R. § 99.3 and "pupil records".

¹¹ *Id.*

¹² Children's Online Privacy: COPPA Compliance | Practical Law, *supra* note 2.

Security Requirements

School boards are mandated to adopt confidentiality policies for pupil records.

Notice & Privacy Policies

While there is no specific notice requirement, policy adoption for record confidentiality is required.

Parent/Student Rights

Parents and students have the right to access and copy progress and behavioral records. Review of behavioral records must include a qualified person to explain the contents.

Access Permitted For

Access to pupil records is permitted for licensed staff, school officials with a legitimate interest, those with court orders, law enforcement, individuals with written consent, in emergencies, and for DCF caseworkers if related to education.

Confidentiality

Pupil records are confidential unless disclosure is allowed by statute.

Service Providers

There is no statutory guidance or contract requirements for third-party vendors in Wisconsin.¹³

Children's Privacy Legislative Tracker & Trends

The landscape of children's privacy legislation is continually evolving at both the federal and state levels.

Federal Legislation

- **COPPA 2.0 (S. 836):** Proposed legislation that would expand protections for teens, broaden the definition of PII, and restrict targeted advertising. NOTE: On **April 22, 2025**, the Federal Trade Commission's (FTC) changes to the Children's Online Privacy Protection Rule (COPPA Rule) were published in the Federal Register.

¹³ *Student Privacy Requirements (WI)*,

<https://plus.lexis.com/document?pdmfid=1530671&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A682G-9C11-F8D9-M3P1-00000-00&pdcontentcomponentid=234344&pdslparesultsdocument=true&prid=03874c5e-30e0-4d78-8a66-7e71b89b1c71&crd=3ab7f4ae-8a52-4d93-8328-69cf674d8a31&pdisdcliderrequired=true&pdpeersearchid=44f7add8-6959-4a74-962d-ef6fc88cad31-1&ecomp=pygg&earg=sr0> (last visited May 30, 2025).

The updates will go into effect on June 23, 2025, and businesses will have until April 22, 2026, to comply.¹⁴

- **Kids Online Safety Act (KOSMA) (S. 278):** A pending bill that aims to limit social media access for minors.

State Legislation Examples

Many states are enacting or proposing new children's privacy laws:

- **Age-Appropriate Design Codes:** California, Maryland, Illinois, New Jersey, and Vermont have implemented or are considering such codes, which require data protection impact assessments (DPIAs), privacy-by-default settings, and restrictions on profiling.
- **Age Verification & Parental Consent:** Arkansas, Connecticut, Georgia, Mississippi, and Virginia have laws or proposals regulating age verification, parental consent, targeted ads, and data minimization.
- **Parental Tools & Opt-Outs:** Nebraska, Wisconsin, and other states have proposed laws featuring parental tools, opt-outs, duties of care, and clearer disclosures.¹⁵

Overall Trends

Several key trends are emerging in children's privacy legislation:

- **Expanded Age Coverage:** Protections are increasingly extending to teens (under 18).
- **Stricter Consent Rules:** There is a move towards more direct consent for teens and requirements for updates when data practice changes occur.
- **Targeted Ad Bans:** Widespread restrictions on behavioral advertising to minors are being implemented.
- **Design & Defaults:** Services are expected to use child-friendly design and privacy-first defaults.
- **Transparency:** Required DPIAs, public reports, and clearer privacy notices are becoming more common.

¹⁴ *FTC Finalizes Amendments to the Children's Online Privacy Protection Rule*, McDERMOTT, <https://www.mwe.com/insights/ftc-finalizes-amendments-to-the-childrens-online-privacy-protection-rule/> (last visited May 30, 2025).

¹⁵ US Children's Privacy Legislation Tracker | Practical Law, *supra* note 6.

- **Minor & Parent Rights:** Enhanced rights for minors and parents to access, delete, and control data are a growing focus.
- **Algorithm Oversight:** Laws are beginning to include opt-outs for personalized content and limits on algorithmic use for minors.¹⁶

What to Expect – Enforcement, Risks & Takeaways

Regulatory Focus

The FTC and state authorities are significantly increasing their enforcement efforts regarding children's data. Non-compliance can lead to substantial fines, investigations, or lawsuits. Adhering to industry guidelines, such as the Student Privacy Pledge, can help demonstrate good faith compliance.¹⁷

Emerging Risks

New technologies present evolving risks:

- **AI, EdTech, IoT:** These sectors involve high data volumes, new risks, and rapidly changing rules.
- **Third-Party Vendors:** Operators bear the responsibility of ensuring their partners' compliance.
- **Patchwork Laws:** The varying rules across different states necessitate careful and comprehensive compliance planning.¹⁸

Practical Takeaways for Attorneys

To effectively advise clients in this complex area, attorneys should:

- Conduct regular reviews of privacy law applicability (COPPA and state laws).
- Monitor new legislation and rulemaking, including updates to COPPA.
- Assist clients in building strong data governance policies and training staff.
- Ensure privacy protections are included in vendor contracts.
- Advocate for privacy-by-design principles in all child-facing products.

¹⁶ FTC Finalizes Amendments to the Children's Online Privacy Protection Rule, *supra* note 14.

¹⁷ Children's Online Privacy: COPPA Compliance | Practical Law, *supra* note 2.

¹⁸ Children's Online Privacy Protection Act (COPPA) Compliance Checklist | Practical Law, *supra* note 1.

- Consider advising clients to explore FTC Safe Harbor programs for added protection.
- Encourage regular auditing of compliance practices.

Resources

- *Children's and Student Privacy Laws Toolkit | Practical Law*,
[https://1.next.westlaw.com/Document/Idfca37b5b07411ee8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DIdfca37b5b07411ee8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=4&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=\(sc.Search\)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD](https://1.next.westlaw.com/Document/Idfca37b5b07411ee8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DIdfca37b5b07411ee8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=4&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD) (last visited May 9, 2025).
- *Children's Online Privacy Protection Act (COPPA) Compliance Checklist | Practical Law*,
[https://1.next.westlaw.com/Document/I5f5954321c8a11e38578f7ccc38dcbee/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI5f5954321c8a11e38578f7ccc38dcbee%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=2&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=\(sc.Search\)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD](https://1.next.westlaw.com/Document/I5f5954321c8a11e38578f7ccc38dcbee/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI5f5954321c8a11e38578f7ccc38dcbee%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=2&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD) (last visited May 9, 2025).
- *Children's Online Privacy: COPPA Compliance | Practical Law*,
[https://1.next.westlaw.com/Document/I5f7b8998bc3f11e398db8b09b4f043e0/View/FullText.html?originationContext=document&vr=3.0&rs=cb1t1.0&transitionType=DocumentItem&contextData=\(sc.Search\)+& IrTS=20250530193312521](https://1.next.westlaw.com/Document/I5f7b8998bc3f11e398db8b09b4f043e0/View/FullText.html?originationContext=document&vr=3.0&rs=cb1t1.0&transitionType=DocumentItem&contextData=(sc.Search)+& IrTS=20250530193312521) (last visited May 30, 2025).
- *FTC Finalizes Amendments to the Children's Online Privacy Protection Rule*, McDermott, <https://www.mwe.com/insights/ftc-finalizes-amendments-to-the-childrens-online-privacy-protection-rule/> (last visited May 30, 2025).
- *Student Privacy Requirements (WI)*,
<https://plus.lexis.com/document?pdmfid=1530671&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A682G-9C11-F8D9-M3P1-00000-00&pdcontentcomponentid=234344&pdislparesultsdocument=true&prid=03874c5e-30e0-4d78-8a66-7e71b89b1c71&crd=3ab7f4ae-8a52-4d93-8328-69cf674d8a31&pdisdocsliderrequired=true&pdpeersearchid=44f7add8-6959-4a74-962d-ef6fc88cad31-1&eomp=pygg&earg=sr0> (last visited May 30, 2025).

- *Student Privacy: Education Service Provider Requirements | Practical Law*,
[https://1.next.westlaw.com/Document/laa4293eea8ee11e598dc8b09b4f043e0/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3Dlaa4293eea8ee11e598dc8b09b4f043e0%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=6&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=\(sc.Search\)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD#co_anchor_a000065](https://1.next.westlaw.com/Document/laa4293eea8ee11e598dc8b09b4f043e0/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3Dlaa4293eea8ee11e598dc8b09b4f043e0%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=6&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD#co_anchor_a000065) (last visited May 9, 2025).
- *US Children's Privacy Legislation Tracker | Practical Law*,
[https://1.next.westlaw.com/Document/I23de7479aee411ee8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI23de7479aee411ee8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=9&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=\(sc.Search\)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD](https://1.next.westlaw.com/Document/I23de7479aee411ee8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89cd9100000196b64adf3733db1305%3Fppcid%3Dad9f9eb9f59c4d0ca071bb4a2231a4f7%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI23de7479aee411ee8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=2af8cec92fd4f0129ce330182b466926&list=KNOWHOW&rank=9&sessionScopelId=dfa2d75b86f57f99e459838192320de8677cf4544ffcbea41d35f331721ba6e8&ppcid=ad9f9eb9f59c4d0ca071bb4a2231a4f7&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&navId=46AEE7E4DFC67C0589D5650FFF31DEDD) (last visited May 9, 2025).



Children's Data Privacy: Navigating Legal and Regulatory Landscapes

June 2025

Ryan Johnson, FIP
Chief Privacy Officer
Vice President
Associate General Counsel
Savvas Learning Co.

Disclaimer: This presentation is for informational and educational purposes only and does not constitute legal advice. Laws and regulations in this area are complex and may change. The presenter is speaking in a personal capacity, and the views expressed do not represent Savvas Learning Company.

© Savvas Learning Company LLC Proprietary & Confidential Information

1

COPPA Overview – Purpose & Scope

- **Purpose:**
 - Children's Online Privacy Protection Act (COPPA) and the Federal Trade Commission's (FTC) implementing rule (COPPA Rule) aim to provide enhanced privacy protections for children under 13 online. **53% of students use GenAI tools regularly**
- **Applicability:**
 - Subject to COPPA if site operator collects personal information from or about users and site/service directed to children <13. Including a broad range of network-connected products and services, such as:
 - Mobile Apps
 - Network connected video games
 - Social Media sites
 - Platform operators w/ **actual knowledge** of child-directed content
- **Personal Information:** Info collected from a child online identifying child or parents, persistent identifiers, biometric & geolocation data
- **Collection Methods include:**
 - Requesting, prompting, or encouraging users to submit information.
 - Passive tracking (cookies, identifiers)

© Savvas Learning Company LLC Proprietary & Confidential Information

2

2

COPPA - Key Concepts & Compliance Basics

- **Lack of Legal Capacity to Consent:** children may not understand consequences of sharing PI and lack capacity to consent.
- **Core COPPA Requirements:** Operators subject to COPPA must comply w/ requirements related to parental notice and obtaining verifiable parental consent before collecting, using, or disclosing personal information from children.
- **Required Privacy Policy Disclosures:** The privacy policy must describe:
 - Data elements collected from children and how it is collected (e.g., directly, passive tracking).
 - Whether children can make personal information publicly available.
 - How the company may use children's information.
 - Practices for disclosing information, types of information disclosed, and 3rd party use it.
 - 3rd Part Sharing: **Who**, **What** (categories of data), and **How** (data retention practices).
 - Procedures for parents to exercise their rights.
- **Privacy Policy Placement:** Clear, prominently labeled PP links on home/landing page, near all data collection points; visibility in mobile apps (app store + in-app) with distinct formatting
- **Parental Access and Control:** Parents have rights to access and control their children's information. (2025)

COPPA - Updates

- **Key FTC Updates include :**
 - **Expanded Age Coverage:** Extends protections to teens aged 13–16, allowing them to consent or exercise rights in certain cases.
 - **Broader PI Definition:** Includes persistent identifiers, photos, videos, audio, geolocation, and biometric data.
 - **Updated "Actual Knowledge":** May include knowledge implied from objective circumstances.
 - **"Directed to Children" Test:** Based on totality of circumstances, including audience data and intent.
 - **Targeted Ads Ban:** Prohibits use of children's or teens' data for targeted advertising.
 - **Data Minimization:** Limits collection to what's contextually necessary.
 - **Notice & Consent:** Requires direct notice and new consent for material changes; bans foreign data transfers without notice.
 - **Enhanced Rights:** Adds access, correction, deletion, and data source/purpose transparency.
 - **Retention Limits:** Data must not be kept longer than necessary for its intended purpose.
 - **Deletion Requirements:** Must delete data when no longer needed or upon parent request; cannot deny service solely due to deletion, with some exceptions.

COPPA - Compliance Measures & Safe Harbor

- **Key Updates Compliance and Security measures include :**
 - **Notice & Consent Alternative:** No consent required if site isn't child-directed and no personal info is knowingly collected.
 - **Data Protection:** Operators must maintain reasonable safeguards, including a written information security program (WISP).
 - **Third-Party Disclosures:** Must vet and obtain written assurances from third parties before sharing children's data.
 - **Third-Party Contracts:** Confirm if partners collect personal info, assess their practices, and limit collection via contract.
 - **Data Retention:** Include a written policy in the privacy notice; delete data when no longer needed or upon parental request, using secure disposal methods.
 - **Ongoing Compliance:** Regularly review policies, consent methods, and vendor practices; audit data handling and parental access compliance.
 - **Safe Harbor Option:** Join an FTC-approved program as an alternative to direct enforcement.
 - Examples of Programs: CARU, ESRB, TRUSTe, Privo, iKeepSafe, kidSAFE.
 - **2025 Updates:** FTC may begin publicly posting certain Safe Harbor operator submissions.

Student Data Privacy Regulation - Federal Laws

- **K12 Data: Requires stronger protections than adults:** EdTech providers must follow federal/state laws and industry standards.:
 - **FERPA:** Governs privacy of student education records.
 - Applies to schools and third-party providers handling student data.
 - Limits access/disclosure; usually requires written consent for sharing PII.
 - DOE offers guidance for service providers.
 - **PPRA:** Covers surveys, marketing, and notice requirements.
 - Applies to third-party providers.
 - Annual and event-based notices must go to parents; providers must inform schools of relevant activities.
 - **COPPA:** Applies to online data collection from children under 13.
 - Requires privacy notices, parental consent, and options for access and control.

FERPA vs. COPPA - Key Differences & Overlap

Purpose:

- **FERPA:** Protects privacy of student education records.
- **COPPA:** Protects PII collected online from children <13.

Applies To:

- **FERPA:** Schools, school districts, and third-party service providers acting on their behalf.
- **COPPA:** Website and app operators directed to children <13 or with actual knowledge of such users.

Consent Required:

- **FERPA:** Requires **written parental consent** for disclosure of PII in education records.
- **COPPA:** Requires **verifiable parental consent** before collecting personal information from children <13.

When Consent Is Not Required:

- **FERPA:** School can share data with third-party providers under a written agreement for educational purposes.
- **COPPA:** No consent required if a school authorizes use of an edtech tool for educational purposes (school acts as intermediary).

Common Misunderstanding:

- Schools authorizing edtech tools **do not always need to collect COPPA consent** separately if doing so under FERPA-compliant agreements.

© Savvas Learning Company LLC Proprietary & Confidential Information

7

7

Student Data Privacy - FTC Guidance & State Laws

- **FTC EdTech Guidance:**
 - Limit data collection to what's necessary for the activity.
 - Data collected via schools must not be used for marketing.
 - Don't retain children's data longer than needed.
 - Implement reasonable security measures.
 - FTC will closely monitor COPPA compliance in edtech.
- **State Student Privacy Laws:** Often stricter than federal law; vary by state. Common focus areas:
 - **Contracts:** Must include parent rights, data security, and disposal terms.
 - **Security:** Require minimum standards, audits, and breach protocols.
 - **Marketing:** Restrict use of student data for commercial purposes.
 - California Laws: SOPIPA: Ban targeted ads, require security, and mandate deletion upon school request.
 - CA Age-Appropriate Design Code: Applies to services likely used by those under 18.

© Savvas Learning Company LLC Proprietary & Confidential Information

8

8

Enforcement Snapshot - Real-World Examples

YouTube/Google (2019):

- FTC & NY AG fined Google \$170M for COPPA violations.
- YouTube tracked children's viewing history for ad targeting without parental consent.

Epic Games (2022):

- \$275M fine for violating children's privacy, including retention of children's data without consent.

Edmodo (2023):

- \$6M settlement for collecting student data without proper parental consent and retaining it beyond what was needed.

Key Takeaway:

- Penalties are significant.
- FTC is actively enforcing children's privacy laws.
- Contracts and policies must reflect compliant data collection, use, and deletion practices.

Student Data Privacy – Wisconsin

- **Key Statutes:** Wis. Stat. § 118.125 (Pupil Records) & § 115.297
- **Covered Entities:** Public K–12 schools and districts (no provisions for third-party vendors)
- **Covered Students:** K–12 students under § 118.125; university students under § 115.297
- **Pupil Records:** Records related to individual students maintained by schools; excludes personal notes, psychological treatment records, and law enforcement records
- **Student Data:** Defined as “education records” per 34 C.F.R. § 99.3 and “pupil records”
- **Security Requirements:** School boards must adopt confidentiality policies for pupil records
- **Notice & Privacy Policies:** No specific notice requirement; policy adoption required for record confidentiality
- **Parent/Student Rights:**
 - Right to access and copy progress and behavioral records
 - Behavioral record review must include a qualified person to explain contents
- **Access Permitted For:**
 - Licensed staff, school officials with legitimate interest, court orders, law enforcement, written consent, emergencies, and DCF caseworkers if related to education
- **Confidentiality:** Pupil records are confidential unless disclosure is allowed by statute
- **Service Providers:** No statutory guidance or contract requirements for third-party vendors

Student Data Privacy – Wisconsin Cont'd

- **Key Statutes:** Wis. Stat. § 118.125 (Pupil Records) & § 115.297
- **Covered Entities:** Public K–12 schools and districts (no provisions for third-party vendors)
- **Covered Students:** K–12 students under § 118.125; university students under § 115.297
- **Pupil Records:** Records related to individual students maintained by schools; excludes personal notes, psychological treatment records, and law enforcement records
- **Student Data:** Defined as “education records” per 34 C.F.R. § 99.3 and “pupil records”
- **Security Requirements:** School boards must adopt confidentiality policies for pupil records
- **Notice & Privacy Policies:** No specific notice requirement; policy adoption required for record confidentiality
- **Parent/Student Rights:**
 - Right to access and copy progress and behavioral records
 - Behavioral record review must include a qualified person to explain contents
- **Access Permitted For:**
 - Licensed staff, school officials with legitimate interest, court orders, law enforcement, written consent, emergencies, and DCF caseworkers if related to education
- **Confidentiality:** Pupil records are confidential unless disclosure is allowed by statute
- **Service Providers:** No statutory guidance or contract requirements for third-party vendors

© Savvas Learning Company LLC. Proprietary & Confidential Information

11

11

Children's Privacy Legislative Tracker & Trends

Federal:

- *COPPA 2.0 (S. 836)*: Expands protections for teens, broadens PII, restricts ads.
- *KOSMA (S. 278)*: Limits social media access for minors (pending).

States (Examples):

- *CA, MD, IL, NJ, VT*: Age-Appropriate Design Codes – require DPIAs, privacy-by-default, restrict profiling.
- *AR, CT, GA, MS, VA*: Laws or proposals regulating age verification, parental consent, targeted ads, and data minimization.
- *NE, WI, others*: Proposed laws with parental tools, opt-outs, duty of care, and clearer disclosures.

Overall Trends:

- **Expanded Age Coverage:** Protections now often extend to teens (under 18).
- **Stricter Consent Rules:** More direct consent for teens; updates required for data practice changes.
- **Targeted Ad Bans:** Widespread restrictions on behavioral advertising to minors.
- **Design & Defaults:** Services must use child-friendly design and privacy-first defaults.
- **Transparency:** Required DPIAs, public reports, and clearer privacy notices.
- **Minor & Parent Rights:** Enhanced rights to access, delete, and control data.
- **Algorithm Oversight:** Opt-outs for personalized content; limits on algorithmic use for minors.

© Savvas Learning Company LLC. Proprietary & Confidential Information

12

12

What to Expect – Enforcement, Risks & Takeaways

Regulatory Focus:

- FTC and states ramping up enforcement on children's data.
- Non-compliance may lead to fines, investigations, or lawsuits.
- Industry guidelines (e.g., Student Privacy Pledge) can help demonstrate good faith compliance.

Emerging Risks:

- **AI, EdTech, IoT:** High data volumes, new risks, fast-changing rules.
- **Third-Party Vendors:** Operators must ensure partner compliance.
- **Patchwork Laws:** Varying state rules require careful compliance planning.

Practical Takeaways:

- Conduct regular privacy law applicability reviews (COPPA + state laws).
- Monitor legislation and rulemaking (e.g., COPPA updates).
- Build strong data governance policies and train staff.
- Include privacy protections in vendor contracts.
- Adopt privacy-by-design for all child-facing products.
- Consider FTC Safe Harbor programs for added protection.
- Audit compliance practices regularly.

© Savvas Learning Company LLC. Proprietary & Confidential Information

13

13

- **Thank You**
- **Questions?**

© Savvas Learning Company LLC. Proprietary & Confidential Information

14

14

Resources

1. Children's and Student Privacy Laws Toolkit | Practical Law, (last visited May 9, 2025).
2. Children's Online Privacy Protection Act (COPPA) Compliance Checklist | Practical Law, (last visited May 9, 2025).
3. Student Privacy: Education Service Provider Requirements | Practical Law, (last visited May 9, 2025).
4. US Children's Privacy Legislation Tracker | Practical Law, (last visited May 9, 2025).