Child Privacy: Legislative Approaches

January 10, 2020

FUTURE OF PRIVACY FORUM



Amelia Vance, Director
Tyler Park, Policy Counsel
Jasmine Park, Policy Fellow

FPF's Privacy Legislation Series

- **Goal:** Providing independent practical resources to policy experts working on legislation, in support of a baseline, comprehensive privacy law in the United States
- **FPF's Mission:** Bridging the policymaker-industry-academic gaps in privacy public policy; developing privacy protections, ethical norms, & responsible business practices.

Previous Sessions (*available at* fpf.org/legislative-resources):

- Defining Covered Data
- Scientific Research
- Federal Preemption of State Laws

www.fpf.org
www.fpf.org/legislative-resources

FUTURE OF PRIVACY FORUM

Webinar Agenda

1. Introduction: Children and Data Privacy
2. Potential Risks and Harms
3. U.S. Approach - COPPA
4. Recent Laws and Proposals
5. International Approaches
6. Considerations for Legislative Drafting (Discussion)
7. Avoiding Unintended Consequences

Q&A (20 minutes)
& Recommended Readings

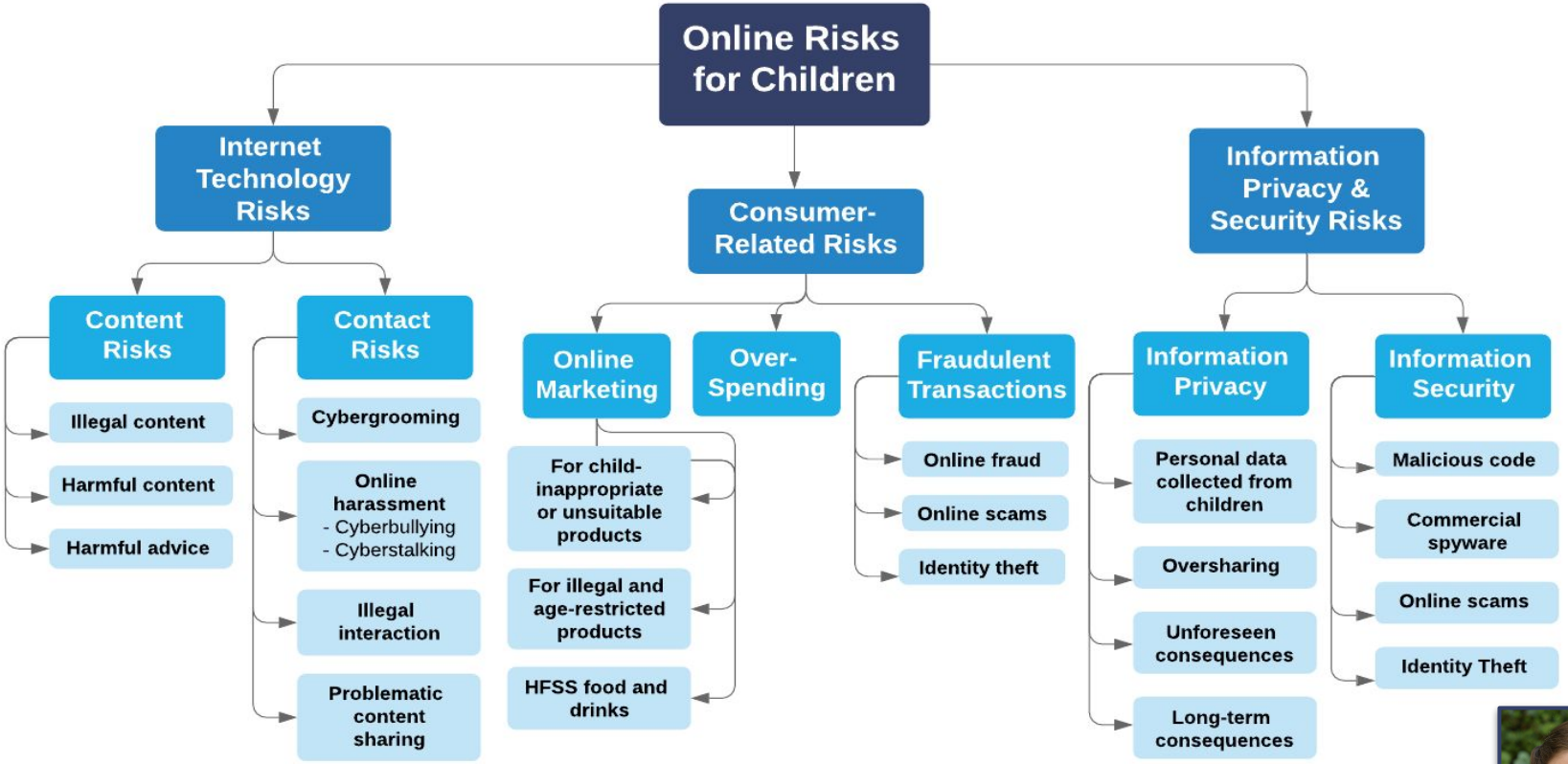
FUTURE OF PRIVACY FORUM

Why Child Privacy Protections?

- **Brains are not fully developed**
  - Unable to fully weigh benefits and risks of data collection and use
  - Limited impulse control
  - Socially vulnerable
- **Lack of experience**
  - Social norms
  - More trusting
- **Potentially more acute harms**
  - Difficulty understand potential future harms
  - Harms may not be fully realized or discovered until later

OECD Typology of Risks

2010



FUTURE OF PRIVACY FORUM

What are you trying to regulate?

Zooming Out On Potential Risks & Harms

- Commercialization
- Age-inappropriate content
- Physical safety
- Loss of opportunity
- Social detriment
- Surveillance acculturation
- Screen time and addiction

US Approaches

US Laws Impacting Children

- Children's Online Privacy Protection Act (COPPA)
- Children's Internet Protection Act (CIPA)
- Family Educational Rights and Privacy Act (FERPA)
- Protection of Pupil Rights Amendment (PPRA)
- California's Eraser Button Law
- State Laws

How Risks are Addressed: COPPA

- Commercialization
- Age-inappropriate content
- Loss of opportunity
- Social detriment

Children's Online Privacy Protection Act (COPPA)

Child Online Privacy Protection Act of 1998 (COPPA)

- Operators must obtain **verifiable parental consent** for the collection, use, or disclosure of personal information from children **under the age of 13**
- Operators must provide parents with types of child's personal information collected and opportunity to prohibit further use or maintenance of child's personal information

FUTURE OF PRIVACY FORUM

US Laws Impacting Children

- Children's Online Privacy Protection Act (COPPA)
- Children's Internet Protection Act (CIPA)
- Family Educational Rights and Privacy Act (FERPA)
- Protection of Pupil Rights Amendment (PPRA)
- California's Eraser Button Law
- Other State Laws

COPPA Amendments and Other Federal Bills

- Do Not Track Kids Act of 2018
- Clean Slate for Kids Online Act of 2019
- H.R.2013 - Information Transparency & Personal Data Control Act
- Preventing Real Online Threats Endangering Children Today (PROTECT Kids Act)

How Risks are Addressed: CIPA

- Age inappropriate content
- Physical safety

How Risks are Addressed: FERPA

- Commercialization
- Loss of opportunity

How Risks are Addressed: PPRA

- Age inappropriate content
- Social detriment

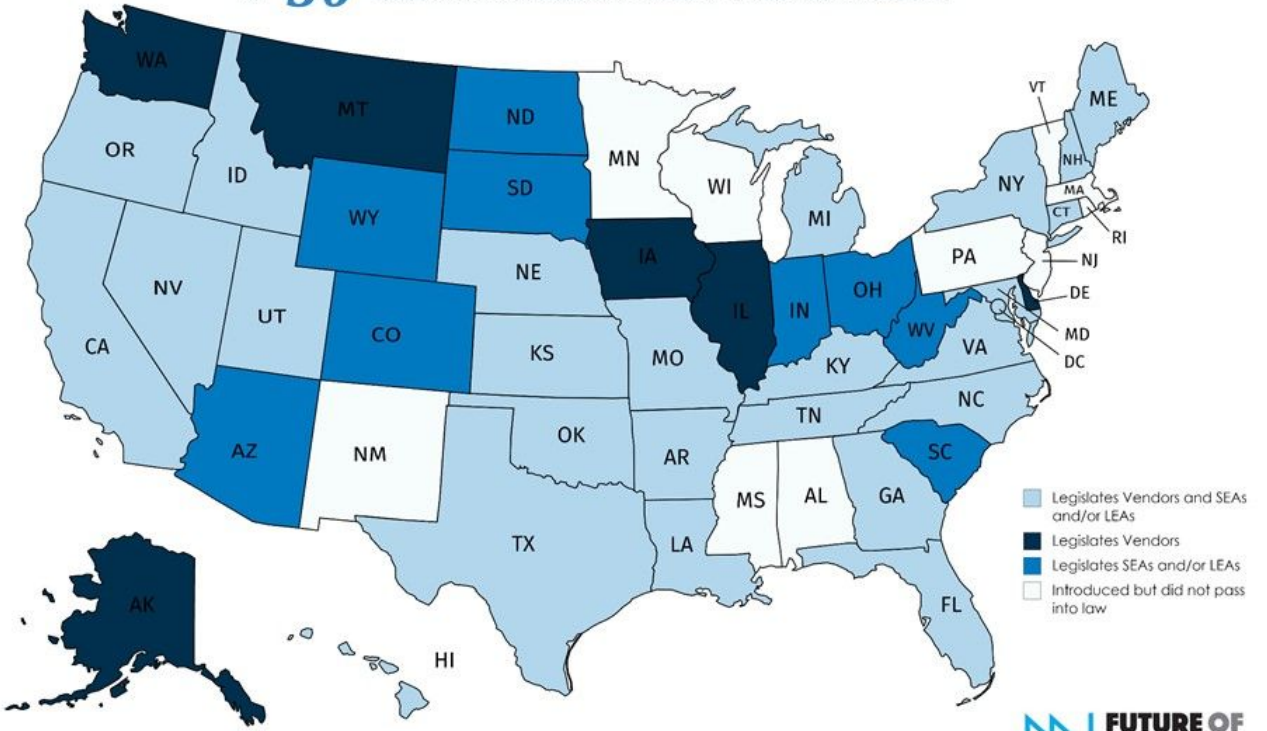
How Risks are Addressed: CA Eraser Button Law

- Commercialization
- Loss of opportunity
- Social detriment
- Surveillance acculturation

FUTURE OF PRIVACY FORUM

41 States Have Passed 126 Laws Since 2013*

All 50 States Have Introduced a Student Privacy Law Since 2013



*170+ laws mentioning student privacy were passed since 2013, but the map above only includes laws that are primarily about student privacy or had significant student privacy provisions

FUTURE OF PRIVACY FORUM

https://ferpasherpa.org/state-laws

How Risks are Addressed: CCPA

- Commercialization

Emerging State Privacy Laws and Federal Proposals

California Consumer Privacy Act of 2018

- Came into effect January 1, 2020
- Opt-in rights for teens between ages of 13 and 16
- Upcoming: **California Privacy Rights Act** of 2020 (CCPA 2.0)

Federal and State Proposals

- Alternative state law approach: “sensitive data” categorization
- Senator Wicker’s Discussion Draft

FUTURE OF PRIVACY FORUM

International Approaches

How Risks are Addressed: GDPR

- Commercialization
- Loss of opportunity
- Social detriment

EU Approach: General Data Protection Regulation (GDPR)

- Came into effect **May 2018**
- Covers entities based in the EU and processing data of people in the EU
- Data Protection Agencies (DPAs) can issue fines up to **€20M** or **4% of annual revenue** for violations

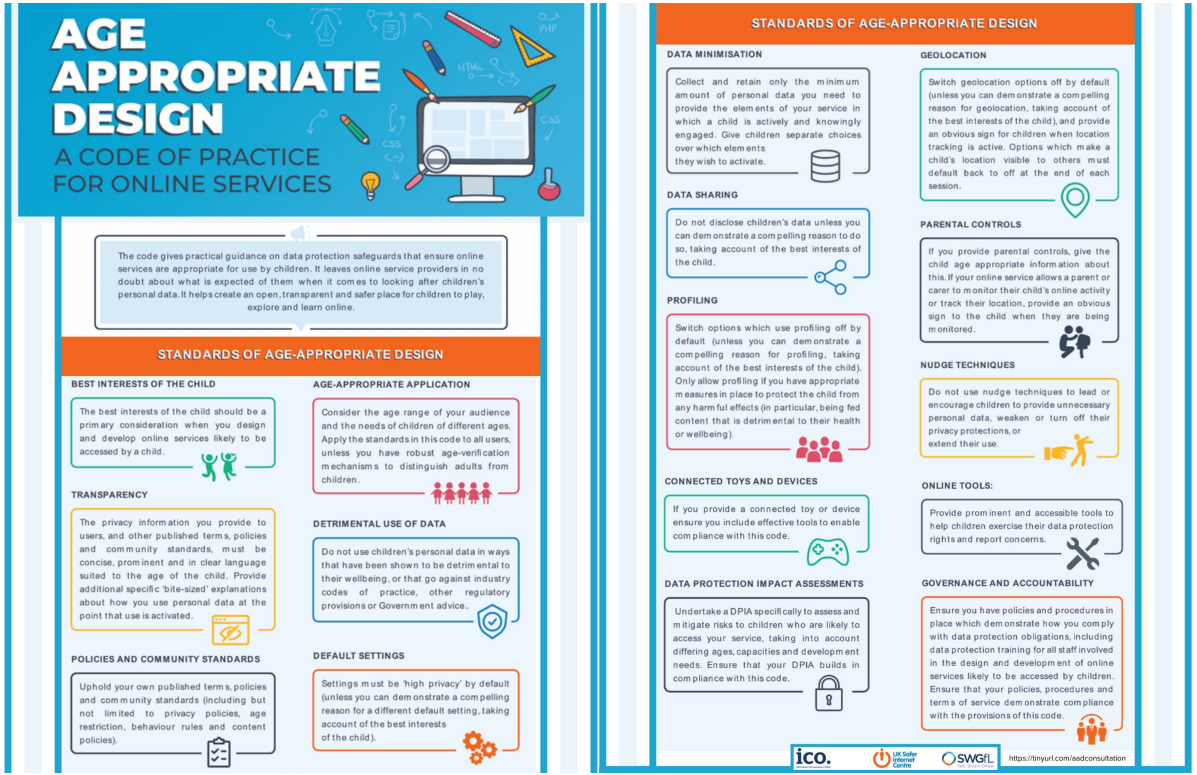
Requires **verifiable parental consent** for processing personal data of children **under the ages of 13 to 16**, depending on the member state, **child-friendly language** for notices provided to children, particular attention to the **right to erasure**, prohibits **solely automated decision making** used on children's data, and provides that children's rights and freedoms **override data controllers' interests** when there is a conflict.

How Risks are Addressed: UK's Age-Appropriate Design Code of Practice

- Commercialization
- Age inappropriate content
- Physical Safety
- Loss of opportunity
- Social detriment
- Surveillance acculturation
- Screen time and addiction

FUTURE OF PRIVACY FORUM

UK's Age Appropriate Design Code of Practice



AGE APPROPRIATE DESIGN

A CODE OF PRACTICE FOR ONLINE SERVICES

The code gives practical guidance on data protection safeguards that ensure online services are appropriate for use by children. It leaves online service providers in no doubt about what is expected of them when it comes to looking after children's personal data. It helps create an open, transparent and safer place for children to play, explore and learn online.

STANDARDS OF AGE-APPROPRIATE DESIGN

BEST INTERESTS OF THE CHILD

The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

TRANSPARENCY

The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.

POLICIES AND COMMUNITY STANDARDS

Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

AGE-APPROPRIATE APPLICATION

Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

DETRIMENTAL USE OF DATA

Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice..

DEFAULT SETTINGS

Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

STANDARDS OF AGE-APPROPRIATE DESIGN

DATA MINIMISATION

Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

DATA SHARING

Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

PROFILING

Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

CONNECTED TOYS AND DEVICES

If you provide a connected toy or device ensure you include effective tools to enable compliance with this code.

DATA PROTECTION IMPACT ASSESSMENTS

Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

GEOLOCATION

Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.

PARENTAL CONTROLS

If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

NUDGE TECHNIQUES

Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use.

ONLINE TOOLS:

Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

GOVERNANCE AND ACCOUNTABILITY

Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code.

ico. UK Safer Internet Centre SWGfL https://tinyurl.com/aadconsultation

FUTURE OF PRIVACY FORUM

UNICEF Principles on Children's Online Privacy and Freedom of Expression

Principle 1 Children have the right to privacy and the protection of their personal data

Principle 2 Children have the right to freedom of expression and access to information from a diversity of sources

Principle 3 Children have the right not to be subjected to attacks on their reputation

Principle 4 Children's privacy and freedom of expression should be protected and respected in accordance with their evolving capacities

Principle 5 Children have the right to access remedies for violations and abuses of their rights to privacy and free expression, and for attacks on their reputation

Recommendation of the OECD Council on the Protection of Children Online

Principle 1 Empowerment

- Policies should empower children and parents to evaluate and minimize risks and engage online in a secure, safe, and responsible manner

Principle 2 Proportionality and Fundamental Values

- Policies should be proportionate to the risks and not restrict the opportunities and benefits of the Internet for children
- Policies should uphold fundamental democratic values of freedom of expression, privacy protection, and the free flow of information

Principle 3 Flexibility

- Policies should be age-appropriate and accommodate developmental differences and special vulnerabilities

How Risks are Addressed: Korean Cinderella Law

- Social detriment
- Screen time and addiction

Korean Youth Protection Revision Act
“Cinderella Law” or “Shutdown Law”

- Requires parental consent for children under the **age of 16** to access gaming websites
- Prohibits children under the age of from playing online video games between **midnight and 6AM**

FUTURE OF PRIVACY FORUM

Considerations for Legislative Drafting

Child Privacy: Potential Risks & Harms Addressed in Law	COPPA (U.S.)	CIPA (U.S.)	CA Eraser Button Law (U.S.)	CCPA (U.S.)	GDPR (E.U.)	Age-Appropriate Design Code (U.K.)	Cinderella Law (S. Korea)
Commercialization	X			X	X	X	
Age-inappropriate content	X	X				X	
Physical safety		X				X	
Loss of opportunity			X		X	X	
Social detriment	X		X		X	X	X
Surveillance acculturation						X	
Screen time and addiction						X	X

What are the limits of regulating child privacy?

Child Online Protection Act of 1998 (COPA)

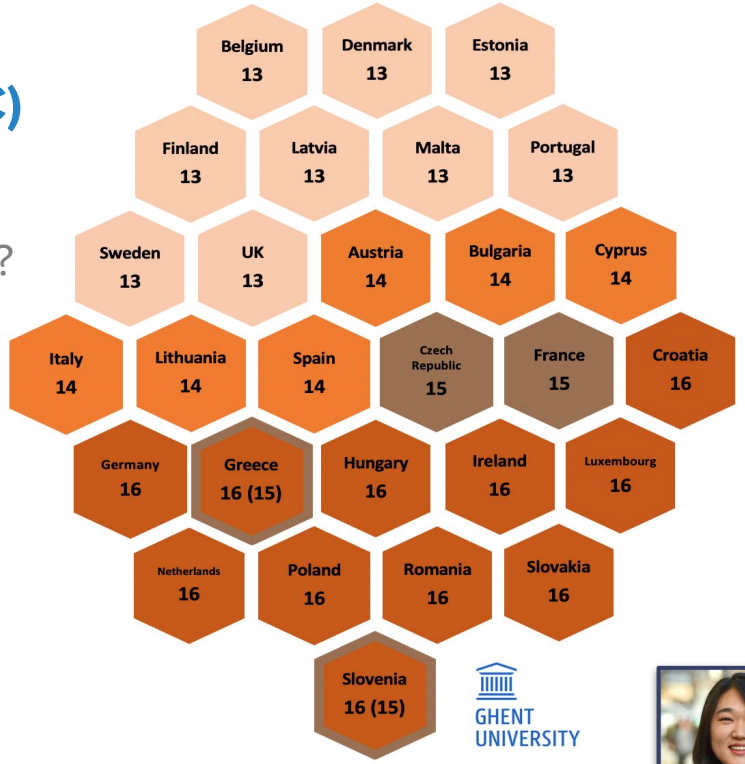
- Intended to criminalize publishing content “harmful to minors” online
- *Ashcroft v. ACLU* (2002)
  - Failed “narrowly tailored” test
  - Age verification
  - Filtering and blocking software

When is consent appropriate?

- Under **COPPA**, parents/legal guardians must opt-in for the collection of data for children **under 13**
- Under **CCPA**, minors **between 13 and 15** must opt-in for sale of their data, parent/legal guardians must opt-in for children **under 13**
- **Possible Alternatives**
  - **Age-Gate** - require age verification prior to accessing service
  - **Signpost** - segment traffic by age
  - **Privacy by Design** - build in privacy at every stage of product development
  - **Age Bands** - develop different versions of product or service for defined age bands, ranging from infancy to adulthood

What is appropriate for different ages?

- **Higher Age (16 GDPR, 18 UK AADC)**
  - Extends protection
  - Parental access? Deletion? Portability?
- **Lower Age (13 COPPA)**
  - Promotes participation
  - Encourages development of digital media literacy and resilience



GHENT UNIVERSITY

FUTURE OF PRIVACY FORUM

What about “age gates?”

With an age gate, children either…

- tell the truth about their age and *retain child privacy protections*, but *lose access to online services* or;
- lie about their age and *retain access to online services*, but *lose child privacy protections*

FUTURE OF PRIVACY FORUM

Avoiding Unintended Consequences

- **Checking with key stakeholders** - such as children themselves, parents, school superintendents (AASA) and attorneys (COSA), the National Center for Youth Law and other child advocates - and from schools, districts, and child welfare organizations
- **Clear definitions**
- **Regulation of "service providers"** (edtech companies) serving public entities (schools)
- **Overbroad exemptions** for existing federal laws
  - e.g. data vs. entities regulated by FERPA or COPPA
- **Preemption** of 150+ state laws

FUTURE OF PRIVACY FORUM

Questions?

Questions about FPF's Legislation Series?

Email us at info@fpf.org

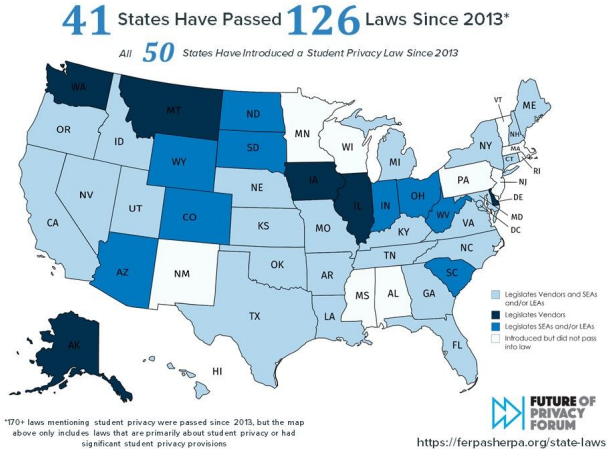
www.fpf.org/legislative-resources

www.fpf.org
facebook.com/futureofprivacy
@futureofprivacy

FUTURE OF PRIVACY FORUM

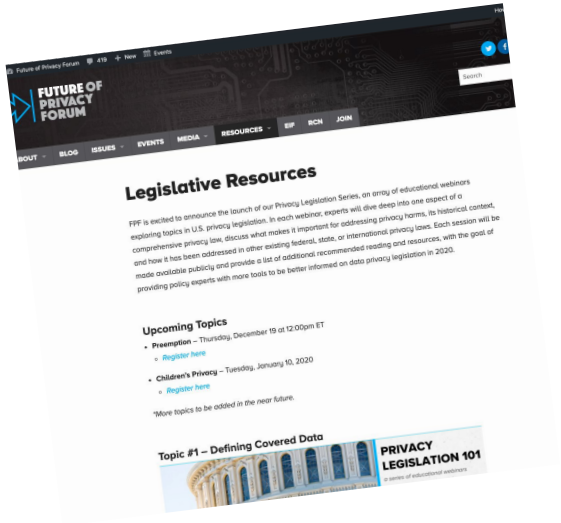
FPF Resources

FERPA SHERPA



FUTURE OF PRIVACY FORUM

Recommended Reading



- The Protection of Children Online, OECD (2012)
- Age Appropriate Design Code Consultation Document, UK ICO (April 2019)
- Industry Toolkit: Children's Online Privacy and Freedom of Expression, UNICEF (May 2018)
- South Korean Youth Protection Act, Korean Legislation Research Institute (March 2016)
- Jeffrey D. Neuburger, U.S. Supreme Court (Finally) Kills Online Age Verification Law, MediaShift (January 2009)

FUTURE OF PRIVACY FORUM