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](http://www.fpf.org)
[www.fpf.org/legislative-resources](http://www.fpf.org/legislative-resources)
Webinar Agenda

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

Q&A (20 minutes)
& Recommended Readings
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
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.
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
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.
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
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
UK’s Age Appropriate Design Code of Practice
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 16 from playing online video games between midnight and 6AM
Considerations for Legislative Drafting
## Child Privacy: Potential Risks & Harms Addressed in Law

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercialization</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Age-inappropriate content</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Physical safety</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Loss of opportunity</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Social detriment</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Surveillance acculturation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Screen time and addiction</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
What are the limits of regulating child privacy?

Child Online Protection Act of 1998 (COPA)

- Intended to criminalize publishing content “harmful to minors” online
  - 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
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
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
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
FPF Resources

41 States Have Passed 126 Laws Since 2013*

All 50 States Have Introduced at Least One Student Privacy Law Since 2013

*“FPF” laws mandating school privacy were passed since 2013. The map above only includes laws that are primarily about student privacy or had significant student privacy provisions.

https://ferpasherpa.org/state-laws

The Policymaker’s Guide to
STUDENT DATA PRIVACY
Recommended Reading

- The Protection of Children Online, OECD (2012)
- Age Appropriate Design Code Consultation Document, UK ICO (April 2019)
- 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)