Privacy Landscape

2022 A4L Privacy & Interoperability Symposium
April 25, 2022
A ‘moment like no other’: A look at children’s privacy in 2021

Biden’s endorsement could be a game-changer for kids’ privacy legislation
Defining Privacy
Privacy was once misconstrued as being about hiding and secrecy. Now it’s understood to be something much more pressing: power dynamics between the individual, the state and the market. [Data protection] must seek to mitigate the inherent power imbalances between people – and those that collect, process and profit off their data.

- Frederike Kaltheuner
Challenge: Allow Opportunities for Youth Online while Mitigating Risks

- **EDUCATION**
- **CIVIC & POLITICAL PARTICIPATION**
- **IDENTITY EXPLORATION**
- **CREATIVE EXPRESSION**
- **HEALTH & WELL-BEING**
- **PLAY**
- **COMMUNITY BUILDING**

Risks
<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety</td>
<td>Is a stranger or someone dangerous able to communicate with my child or learn where my child lives?</td>
</tr>
<tr>
<td>Over-Collection &amp; Over-Surveillance</td>
<td>How much information is being collected about my child?</td>
</tr>
<tr>
<td>The Permanent Record</td>
<td>Will my child’s mistakes be recorded forever?</td>
</tr>
<tr>
<td>Loss of Opportunity</td>
<td>What information will be used to make determine which opportunities my child doesn’t have access to?</td>
</tr>
<tr>
<td>Equity Concerns</td>
<td>What if the information is biased? What if it is used in an inequitable way? What if my child and I can’t or don’t have access to the information or technology?</td>
</tr>
<tr>
<td>Age-inappropriate Content</td>
<td>Is my child accessing content that isn’t appropriate?</td>
</tr>
<tr>
<td>Social Harm</td>
<td>Is my child being cyberbullied or stigmatized?</td>
</tr>
<tr>
<td>Commercialization</td>
<td>Are companies selling my child’s data or targeting advertising to them?</td>
</tr>
</tbody>
</table>
## OECD 2021 Typology of Risks

### Risks for Children in the Digital Environment

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th>Content Risks</th>
<th>Conduct Risks</th>
<th>Contact Risks</th>
<th>Consumer Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cross-cutting</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Interpersonal,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Institutional &amp;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commercial)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Technology Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(e.g. AI, IoT, Predictive Analytics, Biometrics)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risks on Health &amp;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wellbeing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Risk Manifestations

<table>
<thead>
<tr>
<th>Risk Manifestations</th>
<th>Hateful Content</th>
<th>Hateful Behaviour</th>
<th>Hateful Encounters</th>
<th>Marketing Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harmful Content</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illegal Content</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disinformation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Manifestations</th>
<th>User-generated Problematic Behaviour</th>
<th>Other Problematic Encounters</th>
<th>Security Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disinformation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Public Interest Privacy Consulting
Edge Cases: What is a “typical child”?  

Making assumptions about a child’s:

- living situation
- family makeup
- device/internet access
- socioeconomic status
If you were...

- A child with invisible disabilities
- A child who is LGBTQIA and has a family that would harm or kick them out if they knew
- A child facing abuse at home
- A child with a parent who died from COVID
- A child who is undocumented, or whose family is undocumented
- A child experiencing homelessness
- A child who may not have access to a computer, a tablet, or a phone
- A child who may not have access to the internet or may have metered or slow internet

How does that change your data collection or sharing preferences? What risks could you face if your privacy is violated?
The Next Generation of Child Privacy Protections
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.
When consent might not be appropriate/workable

- Foreign Language App
- Student Grades
- Route
- Student Medical Info
- Free Lunch Data, and Allergies
- Math Games
New Child Privacy Protections

Changes to...

● Age of youth who are protected;
● Knowledge standards; and
● Substantive rights granted

Generally excludes “data regulated by FERPA”
Companies are actively creating ways to track behaviour resulting in thousands of individual data points — that reveal a child’s...

- smoking habits
- sexuality
- illnesses, past, present, and future
- social value
- friendship groups
- break ups
- interests
- heartbeat
- financial status
- mood
- location RIGHT NOW
- views, vulnerabilities and when they are most likely to respond
- searches, likes and posts
- bedtime
Why was the Code developed?

By the time a child is 18 it is estimated that there will be 70000 data points about them.

These companies know your children better than you do.

And they keep and share that information forever (for their own gain).
The Code in Practice (maybe)

What if it looked more like this...?

Give the child or young person the opportunity to self-declare for the purposes of data protection.

We use cookies and other technologies to collect user data from your device, so that:

* We can deliver content and advertising that’s relevant to you
* We give you the best experience
* If you’re under 18, we give you greater protection for your data. Click Accept or read our Under 18s Privacy Policy.

Got it! Accept (Under 18)

GREAT!
Because you are under 18 we have given you EXTRA protection for your data. You can now enjoy our site in PRIVACY.

Do you want to know more?

But when you self-declare SOMETHING ACTUALLY HAPPENS!!
The Age-Appropriate Design Code (UK)

The Code mandates data protection that:

- Provides a high level of privacy by design and default
- Explains the nature of the service in child-friendly language
- Does not exploit children’s data for purposes that aren’t in their best interests
- Does not expose or share their location
- Does not use their data to auto-recommend harmful material
- Does not nudge children to make choices that reduce their privacy
- Upholds the terms and conditions that a child has signed up to
- Provides easy-to-use tools to allow children to exercise their data rights
“Children should be afforded protections not only by digital products and services specifically directed at them, but by all digital products and services they are likely to access.”
The California Age-Appropriate Design Code

A business that provides a good, service, or product feature likely to be accessed by a child shall comply with all of the following:

- Consider the best interests of children
- Undertake a Data Protection Impact Assessment
- Establish the age of consumers with a level of certainty appropriate to the risks that arise from the data management practices of the business, or apply the privacy and data protections afforded to children to all consumers.
- Maintain the highest level of privacy possible for children by default
- Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language
- Provide an obvious signal to the child when they are being monitored or tracked
- Provide prominent, accessible, and responsive tools to help children exercise their privacy rights and report concerns.
The California Age-Appropriate Design Code

A business that provides a good, service, or product feature likely to be accessed by a child shall not take any of the following actions:

- Use the personal information of any child in a way that is demonstrably harmful to the physical health, mental health, or well-being of a child.
- Collect and retain any personal information that is not necessary.
- Use the personal information of a child for any reason other than the reason or reasons for which that personal information was collected.
- Disclose the personal information of any child unless the business can demonstrate a compelling reason.
- Collect any precise geolocation information by default.
- Collect any sensitive personal information by default.
- Use dark patterns.
What’s Next?
Pandemic Repercussions and Lessons Learned

- Data sharing has been shown to be more important than ever - but we also need, more than ever before, to facilitate public confidence in transfers of data.
- The technology adopted during the pandemic is being adapted and reinterpreted for ongoing educational and community use, despite privacy concerns and pushback.
- We’ll need to balance increasing legislatively-imposed sensitive data privacy protections and parent demands for access and control with the increased desire to use data to help students.
  - Combatting learning or social-emotional development losses
  - Providing mental health supports
  - Re-engaging with families whose children disappeared during online classes
Student Privacy Trends

- Interest in child privacy that trickles over to student privacy
- Parents wanting opt-out or opt-in on curricular materials - including edtech!
- Student monitoring
- Social-emotional evaluations
- Early warning systems
- Growth of civil rights organizations in student privacy
- Algorithms in education
- Increased focus on child wellbeing related to digital literacy and privacy education
Where SDPC Comes In
The Landscape Continues to Change, and Legal Compliance is Not Enough
The Problem with a Student Privacy Champion: They Leave
Goal: Cultivating a Culture of Privacy

A culture of privacy within schools means everyone who has access to students’ personal information is trained and know why and how to effectively and ethically collect, use, share, protect, and secure it.
Consortium Goals

1. Develop tools and resources to address operational issues not currently being addressed.

2. Develop a clearinghouse of student data privacy operational issues and resources to support schools, districts, states and vendors in managing those issues - no matter where the resources originate.

3. Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management.

4. Identify projects that have on-the-ground and real-world impact on student data privacy enabling schools, districts, state and vendors find resources, adapt them to their unique context and implement needed protections.

5. Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work.
From Chaos...

...To a System That Lasts