Children's Privacy – Special Considerations

9 May 2024

Marsali Hancock
EP3 Foundation

Katy Ruckle
Washington
State Chief
Privacy Officer

Mandy Cartright
Lewis Brisbois

Chuck Cosson
Seattle University
School of Law

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Marsali Hancock

President and CEO
EP3 Foundation

Katy Ruckle

Washington State
Chief Privacy Officer

Mandy Cartwright

Partner
Lewis Brisbois

Chuck Cosson

Adjunct Professor
Seattle University
School of Law

Key Takeaways – The Entire Panel in One Slide

1) Special protections for children are common in law and regulation, based on differences in children's cognitive development, sensitivity to privacy, safety and dignity harms, and to protect rights of parents
2) Federal law already provides:
    a) Collection of personal data of children <13 requires verifiable parental consent (COPPA)
    b) FTC COPPA Regulation spells out compliance guidance, including methods for verifiable parental consent
3) Federal legislative ideas
    a) COPPA 2.0 legislation – ban targeted advertising to children, raise age to 16, expand scope
    b) KOSA - require platforms to observe a duty of care; require parental notice for youth online accounts
4) State law already provides, among other things:
    a) California CCPA and other states: parental consent required for "sale" of data of persons <13
    b) Several states require opt-in for sale or sharing of data of persons 13-15; treated as "sensitive" data
5) State legislative ideas:
    a) CA Age-Appropriate Design Act – if "likely to be accessed" by children must default to strongest settings
    b) Various proposals to require age verification and/or parental consent for use of social media
6) Special considerations
    a) Laws will need to comport with 1st Amendment (CA AADA struck down on this basis)
    b) Children online also involves security, safety & human rights issues, and necessary trade-offs

Privacy+ Security Forum

Special Considerations for Children

Privacy+ Security Forum

Why treat children's privacy differently?

1997 – FTC investigates "KidsCom" privacy notice; notes children's limited ability to comprehend privacy notices (leads to COPPA)

- Concern = children can't read / comprehend privacy notices. Back when "notice" was the favored solution!

2011- State AGs incentivize creation of expert task force to address sexual solicitation, online harassment, bullying, and online content; consider age verification as a solution.

- Concern = issues beyond notice of data use; include "trust and safety" issues for children and teens.

2013 – FTC expands COPPA

- Concern: maintaining integrity of COPPA protections on notice & choice as technology changes.
- FTC rule change widens the definition of children's personal data to include persistent identifiers (cookies), as well as geolocation, images, & audio.

What are some open issues?

2023 – FTC and Congress both take aim at targeted advertising to children. Concerns include both privacy (excess data collection creates privacy & security risks) & emotional harm (children exposed to manipulative ads).

- Concern = tracking of kids for social media and/or advertising affects their identity, health, and autonomy.
- Concern = design tools built on profiling misuse asymmetric power over child cognition to keep children engaged with apps or to buy products

Illustrated:

- *"Kids must be able to play and learn online without being endlessly tracked by companies looking to hoard and monetize their personal data" - FTC Chair Lina M. Khan.*
- *[This bill] would stop the growing social media health crisis among kids by setting a minimum age and preventing companies from using algorithms to automatically feed them addictive content based on their personal information" – Senator Brian Schatz (D-HI)*

Special Considerations for Children

Federal law on children's privacy

Child's Online Privacy Protection Act (COPPA)

- Notice - Post a privacy notice on practices for personal data of persons < age 13 and make reasonable efforts to directly notify parents of these practices;
- Consent - Obtain verifiable parental consent, with limited exceptions, prior to collection & use of < age 13 user data;
- Access & Control - Provide a reasonable means for a parent to review personal data of their child and to control future use or retention;
- Data Security- Maintain reasonable safeguards for confidentiality, security, & integrity of < age 13 user data;
- Data Minimization - Retain child personal data only as long as needed. COPPA-subject firms may not condition child's participation in an online activity on the child providing more data than is reasonably needed.

Family Educational Rights and Privacy Act (FERPA)

- Protects privacy of students in a public educational context
- Provides rights of parental access to educational records
- Requires written permission from the parent or eligible student to release data from a student's education record (subject to exceptions for health, safety, law enforcement, educational operations, etc.).

Special Considerations for Children

What changes in federal law are proposed?

Kids Online Safety Act (KOSA)

- Response to Meta allegations
- Requires covered firms to provide tools to disable product features and opt out of personalized recommendations;
- Creates a duty for platforms to prevent and mitigate certain dangers, including suicide promotion, eating disorders, etc.;
- Requires covered firms to perform an annual independent audit assessing risks to minors and steps to prevent those harms;
- Provides academics and NGOs access to research data.

American Privacy Rights Act of 2024 (APRA)(discussion draft)

- Leaves COPPA intact but adds protections for a "covered minor" (age 13-17), including treating such data as "sensitive" data;
- Opt-in consent needed for transfer of "sensitive" data to 3rd parties;
- Requires algorithmic impact assessments for online services that process data of covered minors;
- Preempts inconsistent state laws on privacy rules for children.

Special Considerations for Children

What do state laws require for children's privacy?

Some illustrative provisions:

- California Privacy Rights Act adds protections for children:
  - A business cannot sell or share personal data of a child aged 13 to 15 without the affirmative consent of the child;
  - For a child under the age of 13, sale or sharing requires affirmative consent of the child's parent or guardian.
- Kentucky law signed April 2024 is similar:
  - Provides, as do other state laws, that children's data is among the "sensitive" data category;
  - Expressly requires COPPA compliance to process "child" data.

9th Circuit holds COPPA does not preempt consistent state laws

Also, state Attorneys General can enforce COPPA

- WA AG Bob Ferguson fined/settled case with "We Heart It" social media platform for alleged COPPA violations;
- NM AG claim (2020) v. Google for COPPA violations dismissed; Google was entitled to rely on schools with which it contracted to obtain parental consent for processing of student data.

Special Considerations for Children

What changes are likely to occur in state law?

Most new state privacy laws address children's privacy similar to CPRA, Virginia privacy law, etc.

- For example, New MD law (proposed) would treat data of a "child" as "sensitive" data;

But--- States are also attempting to regulate social media & online safety:

- California Age-Appropriate Design statute:
  - Firms must consider the "best interests" of children when designing & providing online service;
  - Means privacy, safety and well-being of children must be prioritized over commercial interests;
- Other states also attempting social media, safety and privacy legislation (more to come…)

Special Considerations for Children

Recent Washington State legislation

SB 6184 - Concerning deepfake artificial intelligence-generated pornographic material involving minors.

SHB 1999 - Concerning fabricated intimate or sexually explicit images and depictions.

Special Considerations for Children

Privacy+ Security Forum

Washington State laws on Ed Tech

Student User Privacy in Education Rights (SUPER act)
Chapter 28A.604 RCW

Special Considerations for Children

Privacy+ Security Forum

Other state laws

Maryland

- New privacy law focuses on data minimization – use only what is "reasonably necessary & proportionate" to provide service requested by consumer to whom the data pertains.
- Kids Code would prohibit certain social media and other online platforms from tracking people under 18 and from using manipulative techniques — like auto-playing videos;

Utah

- Privacy bill similar to Virginia and other state laws; lacks some requirements that are in CPRA, such as right to opt out of profiling. But…
- Utah's Social Media Act would require parental consent for any child < 18 to use the site and proactively verify the age of every user. Also subject to a 1st Amendment challenge.

Florida

- SB 262 signed; becomes effective July 1, 2024
- Similar to other state privacy laws, but also includes terms regulating social media for children (<age 18).
  - Social media platforms with > 5M customers must not process children's data if substantial harm will result;
  - May not "profile" a child unless necessary,
  - May not use child personal data for other than a stated purpose.

Montana

- Privacy bill similar to other states, e.g., data of person <13 is "sensitive data" and COPPA compliance is required
- MT also, somewhat famously, attempted to ban TikTok; that is also enjoined on 1st Amendment grounds

Special Considerations for Children

Privacy+ Security Forum

What must lawmakers take into account in addition to privacy?

1st Amendment

- Requires gov't to meet appropriate level of scrutiny for restrictions of speech
- Such regulations must pass a "means/fit" test – are they tailored to advance government interests, without undue burdens on speech?

Privacy and Youth Autonomy

- Parental consent requirements generally fine but after age 16 policy considerations change as such rules do restrict privacy of youth vis-à-vis their parents

Special Considerations for LBGTQ+ youth

- Parents may not have youth well-being in mind
- Some states may abuse "duty of care" rules

What might courts say about these proposals?

NetChoice v. Bonta

"A law that restricts the "availability and use" of information by some speakers but not others, and for some purposes but not others, is a regulation of protected expression." – N.D. of California, Order granting injunction (September 2023)

Law that restricts the sale and sharing of personal data by certain speakers for certain purposes but not others, is thus a regulation of protected expression.

Court finds regulation of data processing – as distinct from regulation of service design – does not pass the applicable means/fit test. Law is not sufficiently tailored to advance the governments interests in privacy without also harming free speech.

Mandatory Age Verification

- Susceptible to challenge on both means/fit test and on impacts on privacy & speech. May run afoul of case law protecting right to speak anonymously.

Bans on Youth Access to Social Media

Packingham case suggests highest level of scrutiny for such laws may be warranted given the centrality of social media to contemporary life, commerce, etc.

Special Considerations for Children

Privacy, Children and Human Rights

Human Rights Instruments

- Informed the UK Online Safety Act and referenced in state "design code" proposals, e.g. UN Convention on the Rights of the Child
- *But human rights includes more than privacy!*
  - K.U. v. Finland – European Court of Human Rights rules Finland is not in compliance with human rights obligations where it did not allow law enforcement to compel access to personal data;
  - Human rights requires access to remedy for harms to human dignity, e.g., revenge porn, as well as other goals including security and economic opportunity.

Law Enforcement, National Security and CSAM

Encryption

- Various objections to use of "end to end" encryption
  - FBI has referred to this as the "going dark" problem.
  - Redux of the 1990's "crypto wars: e.g., the "Clipper Chip" – which would have created an NSA backdoor to encryption;
  - In 2023 – new concerns that Meta adding encryption to Messenger will enable use to transmit Child Sexual Abuse Material ("CSAM")
- *Which approach favors children's privacy?* **Both do!**
  - Encryption protects personal data against unauthorized interception; includes children on messaging apps;
  - To the extent CSAM is undetected due to encryption, each transmission of CSAM is harmful to children.

Questions for the Panel?

Privacy+ Security Forum

Marsali Hancock

President and CEO
EP3 Foundation

Katy Ruckle

Washington State
Chief Privacy Officer

Mandy Cartwright

Partner
Lewis Brisbois

Chuck Cosson

Adjunct Professor
Seattle University
School of Law

Readings

- COPPA Statute (15 USC 6501 et. seq.)
- COPPA Regulation
- FTC COPPA Rulemaking
- "COPPA 2.0" bill – Markey/Cassidy
- Final Report – Berkman/MySpace Youth Internet Safety Task Force (2009)
- Statement of Meta Whistleblower Frances Haugen – U.S. Senate
- Kids Online Safety Act; Coalition letter on children's privacy legislation
- Protecting Kids on Social Media Act ; Coalition letter
- NTIA Request for Comment on Children's Privacy and Safety issues (October 2023)
- US Surgeon General advisory on youth mental health and social media
- Summary of state laws on children's privacy
- CA Age-Appropriate Design Act; law firm summary; FPF analysis
- Court injunction blocking CA AADA
- IAPP analysis of children's privacy laws and related 1st A implications
- News article on dialogue among online safety regulators
- Kate Hamming, A Dangerous Inheritance: A Child's Digital Identity, 43 SEATTLE U. L. REV. 1033 (2020)