Sociotechnical Security

CS 8803/4803

Professor Veronica Rivera

Lecture 20 – Youth Digital Safety I



Content warning: Brief mentions of CSAM

Last time

- AI-enabled sexual abuse experienced by adults and children
- Proposed solutions and debates
- Overview of policy discussions in the US on AI-enabled sexual abuse
- Discussion

Today

- Introduce digital safety topics around youth safety
- Brief historical context
- Research topics on children’s digital privacy
- Age verification

High-level youth safety topics in digital safety

Youth digital safety is the study of how technology creates and mediates threats to young people's well-being, including physical, emotional, sexual, relational, or financial threats. The field also examines how youth, the adults who support them, and platforms can work together to help youth prevent and/or recover from digital safety harms.

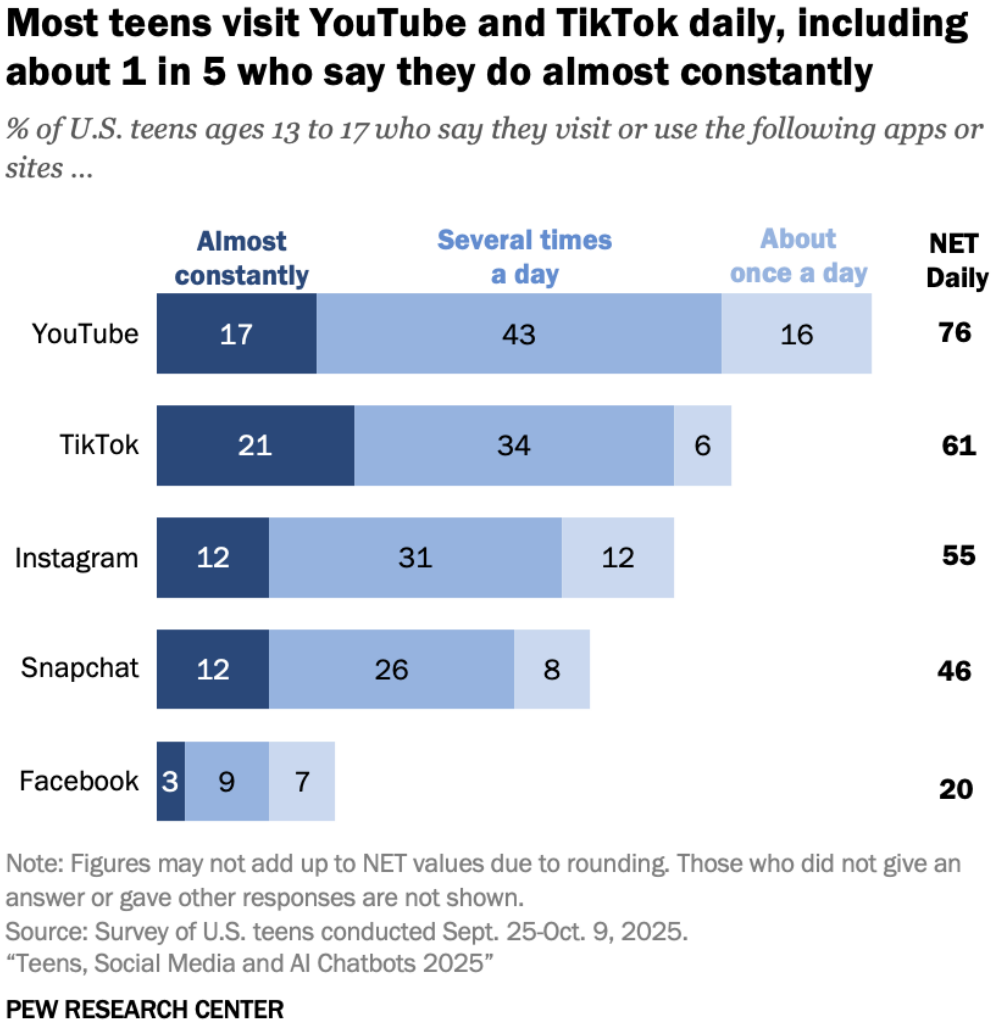
Topics

- Online harms
- Mental health and well-being (esp. related to social media & AI)
- Children's understanding of S&P
- S&P education for kids
- Platforms, products, and policy
- Families and privacy (e.g., sharenting)
- Age verification
- And more…

Youth are increasingly online

In a study from 2025:

- ~75% of US teens surveyed use Youtube every day
- 36% of teens use at least one of TikTok, YouTube, Instagram, Snapchat, and Facebook almost constantly.
- A majority of teens (64%) have used an AI chatbot
  - ~30% everyday
  - ~16% several times a day or almost constantly



(Overly simplified) history of youth digital safety

- Late 1990s – early 2000s: harmful content and kids' data
  - Children's Online Privacy Protection Act (COPPA)
- 2000s: Stranger danger online
  - Predators on myspace-era social networks
- Late 2000s – early 2010s: peer harms
  - Online harassment
  - How kids use social media, challenging common adult myths
- Late 2010s - now: parental mediation & privacy
  - Parental controls vs. kids' autonomy
  - Sharenting
- Early 2020s - now
  - Social media and youth mental health
  - Age verification
  - AI-enabled abuse

Risk categories: The 4Cs of youth digital safety

From London School of Economics' EU Kids Online Project

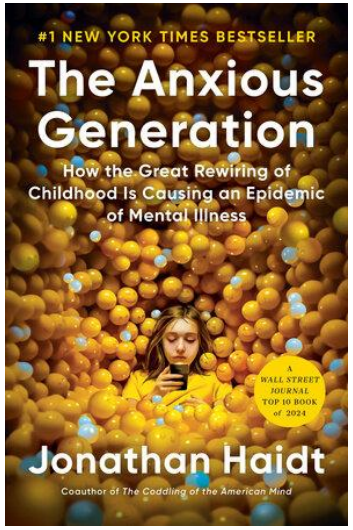
Category	Definition	Examples
1. Content	What children **see** or read online. The child is a passive recipient of harmful material.	Exposure to violence, hate speech, pornography, or fake news.
2. Contact	What children **experience** through communication. Interactive risks initiated by others.	Stranger harassment, cyber-grooming, extortion, or aggressive peer pressure.
3. Conduct	How children **behave** online. The child is an active participant in harmful actions.	Cyberbullying, trolling, or sharing inappropriate/hurtful digital content.
4. Contract (or Commerce)	What digital **agreements** or transactions children enter into.	Hidden in-app purchases, scams, gambling, or platforms exploiting children's data and privacy.

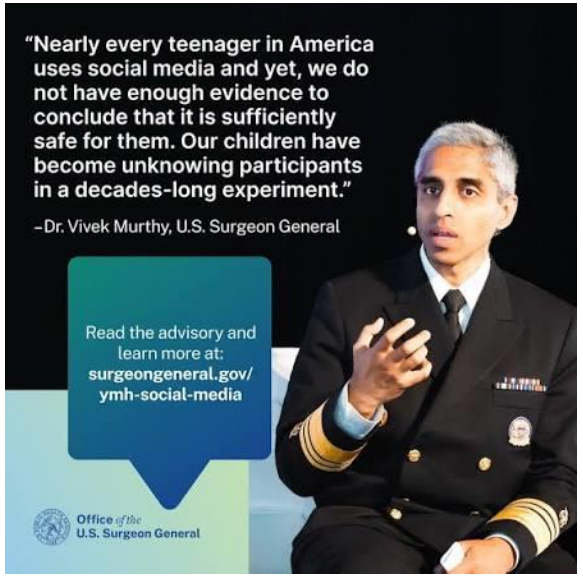
Research topics on children's digital privacy

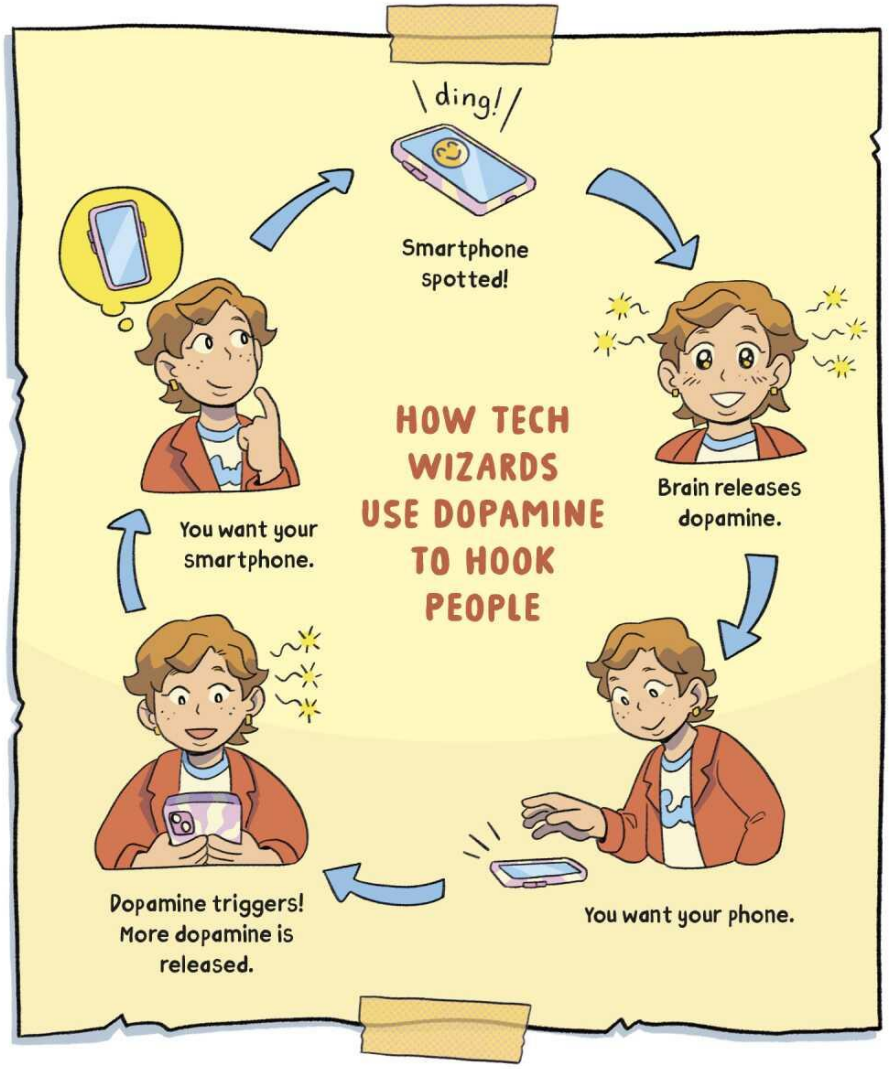
- How children understand privacy
  - Leah Zhang-Kennedy et al., IDC 2016 (You read for today)
- Teens' privacy practices
  - danah boyd, "It's Complicated: the social lives of networked teens", 2014
- Parents as privacy actors
  - Sophie Stephenson et al., CHI 2024 (You read for today)
  - Carol Moser et al., CHI 2017 → children and parents disagree about consent and boundaries
- Commercial data collection
  - Irwin Reyes et al., PETS 2018 → COPPA violations in Android apps
  - Emily McReynolds et al., CHI 2017 → Privacy mental models in connected toys

Social media harms

- Teen anxiety, depression, and self-harm rose in the early 2010s
  - Correlated with smartphones and social media becoming more widespread
- Jonathan Haidt: social media has rewired children's brains →
- Wrote a book on this, naming four harms from social media:
  - Social deprivation, sleep loos, fragmented attention, addiction
- Supporting evidence: Frances Haugen & Facebook files
- US Surgeon General warning

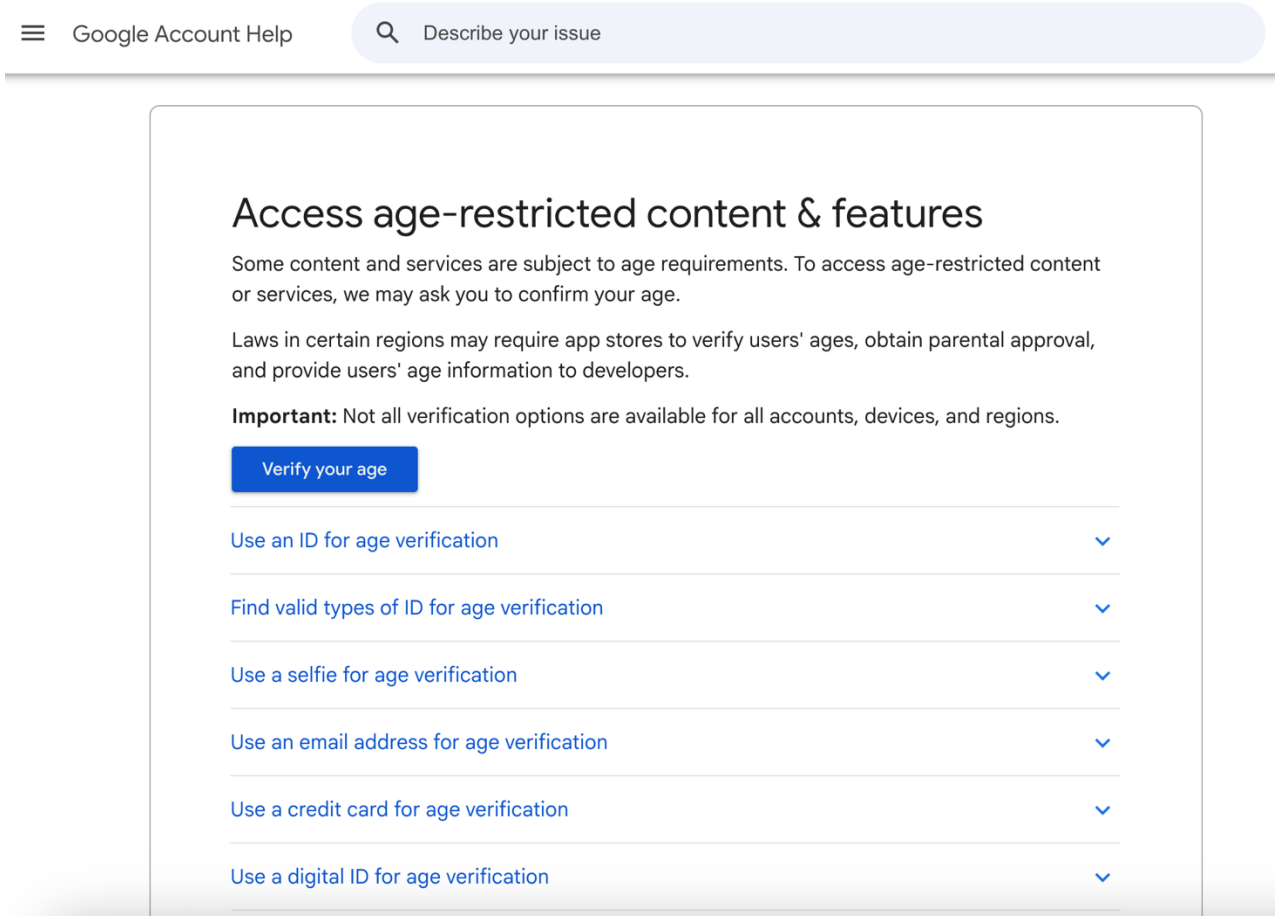






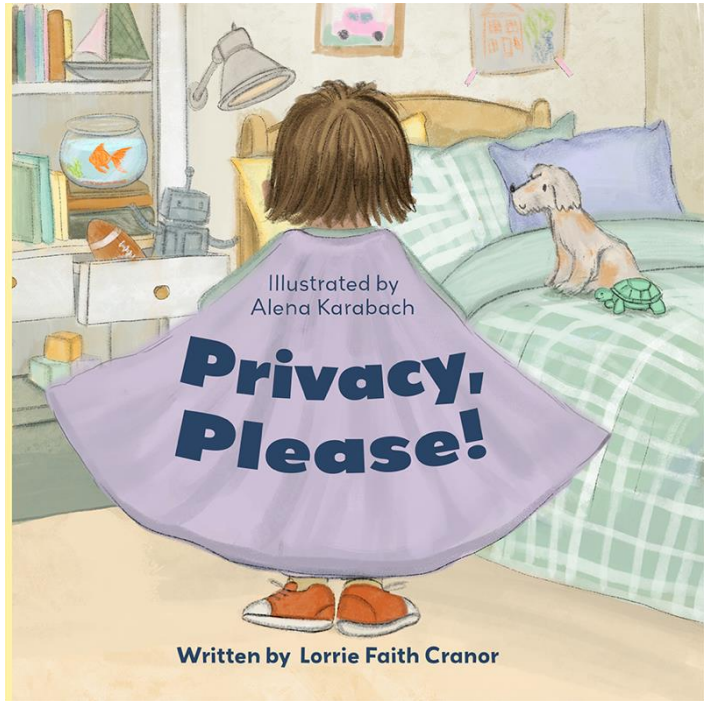
Age verification

- Age verification required in:
  - UK
  - Australia
  - Some US states (implementation varies across states)
- Risks and concerns
  - Data collection from everyone
  - New breach targets
  - Accuracy and bias
  - Easy to evade
  - Access and equity





Helping children understand privacy



- Children's book aimed at helping families talk about personal boundaries, personal independence, and digital safety: Learn more here
- Written by Lorrie Cranor, usable security and privacy professor at CMU
- Grew out of community-based project that had people draw what privacy means to them.
  - See drawings here: https://cups.cs.cmu.edu/privacyillustrated/