What are you most concerned about with your child's internet use?

- Child predators

- Bullying

- Permanence (can't delete/undo embarrassing posts)

- Misinformation and radicalization

- Datamining and privacy compromise

Agenda

- Introduction
- YouTube case study
- Data mining
- Pitfalls of Free speech platforms
- Applications/websites to be mindful of
- Cancel culture: the "worst thing you've ever done"
- Parental pitfalls
- "Best Practices" and monitoring

Agenda

- Introduction

- YouTube case study

- Data mining

- Pitfalls of Free speech platforms

- Applications/websites to be mindful of

- Cancel culture: the "worst thing you've ever done"

- Parental pitfalls

- "Best Practices" and monitoring

- Interrelated causes and issues.

- Understanding the interconnectedness of these topics will help you navigate and mitigate potential harms.

Introduction

- Grew up in Alaska

- B.A. Philosophy, Politics, Economics, and Law from the University of Arizona

- M.S. in Cybersecurity Risk Management from Indiana University Bloomington

- J.D. from Indiana University Maurer School of Law

- Cybersecurity Consultant and General Counsel at Reveal Risk

- Hobbies: spending every minute of my free-time watching Netflix

- Became interested in Children's privacy though my own experiences as a teenage YouTube Vlogger
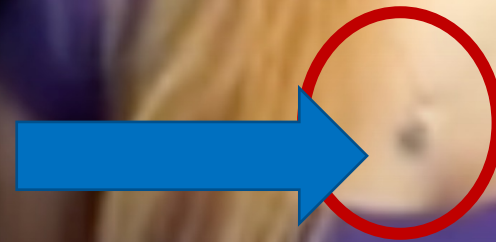
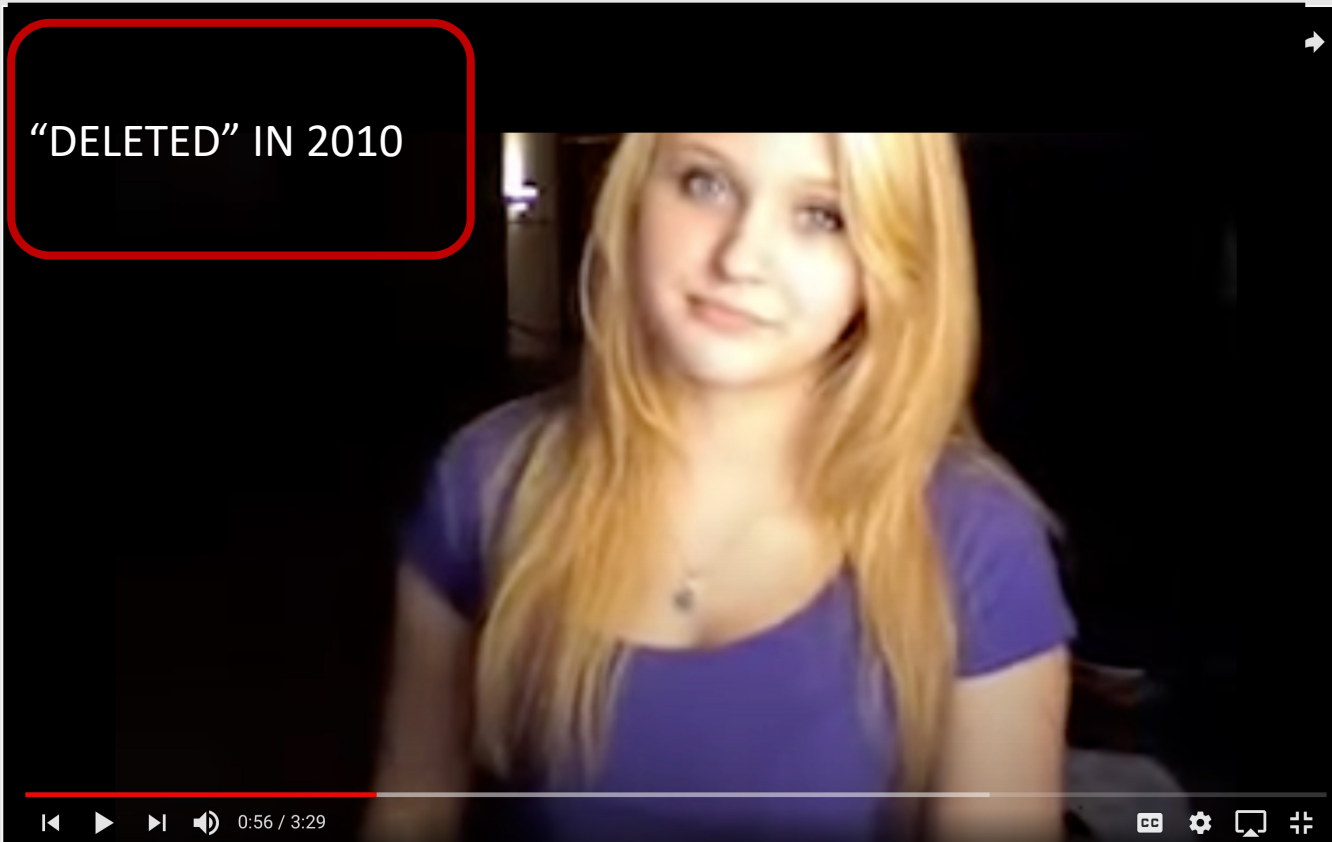15 years old

0:56 / 3:29

REVEALRISK
SECURE YOUR BUSINESS
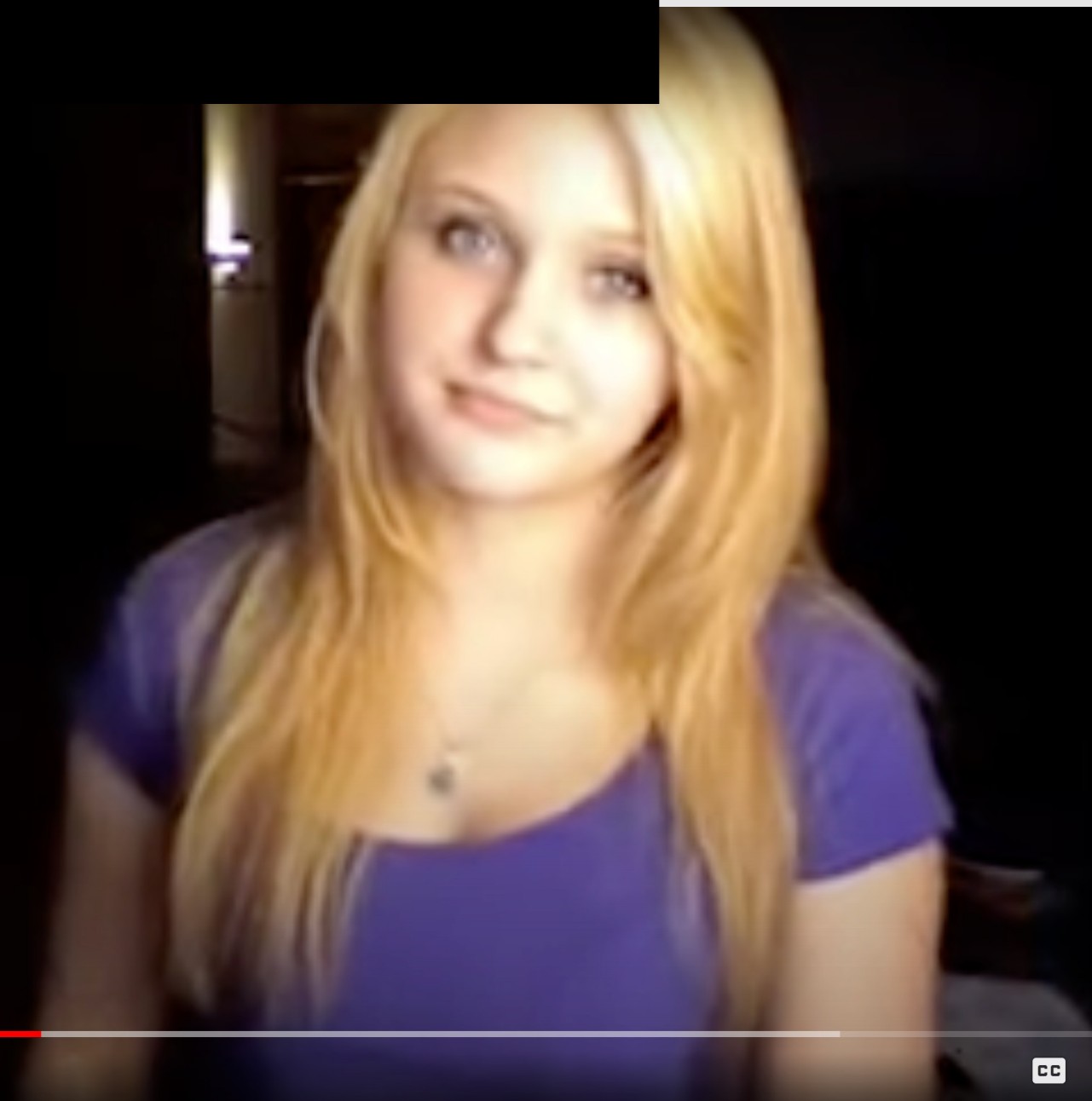
It doesn't go away…


"DELETED" IN 2010

The internet duplicates

- You can still find these videos.
- This isn't "cute" anymore to me and I can't delete it.
- Applications like Snapchat are a lie.

YouTube loves kids

- In 2019 YouTube received backlash for being complicit in its platform's use by child predators. YouTube's "suggested video" algorithm was recommending an unending supply of partially clothed prepubescent children to users who had watched similar videos in the past. Perhaps, more horrifying, they promoted ads and sponsored content to monetize the unwittingly pornographic material uploaded by their young users.

High-level break down

- Algorithm promoted content with child nudity to people who had viewed similar content.

- The comment sections of these videos became forums for pedophiles.

- Pedophiles time-tagged specific instances of child nudity and linked to other videos and external forums.
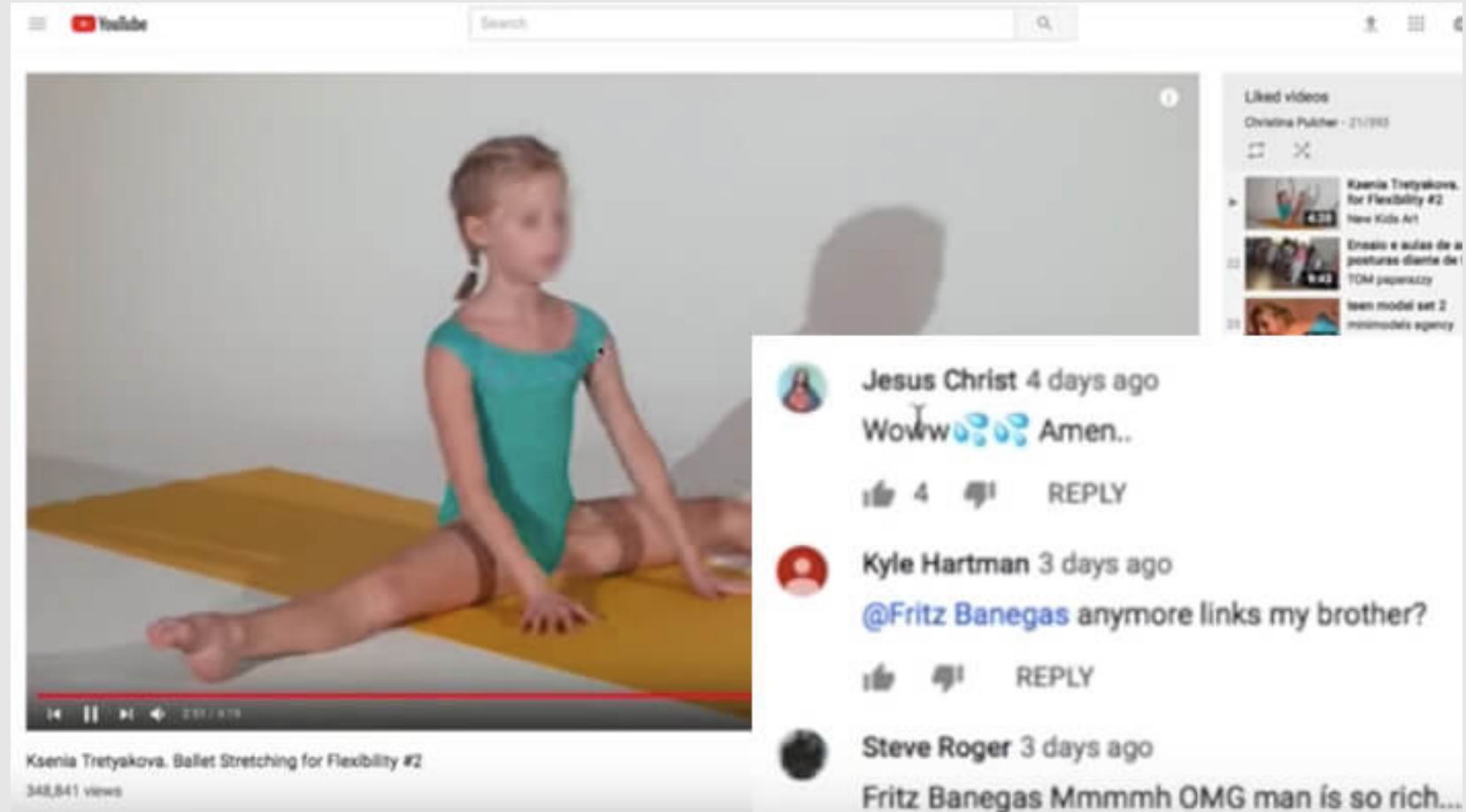
Predatory Time-Tagging

Time tagging: (v) the act of hyperlinking specific parts of videos to link directly to content.

Example: Check out: 0:56
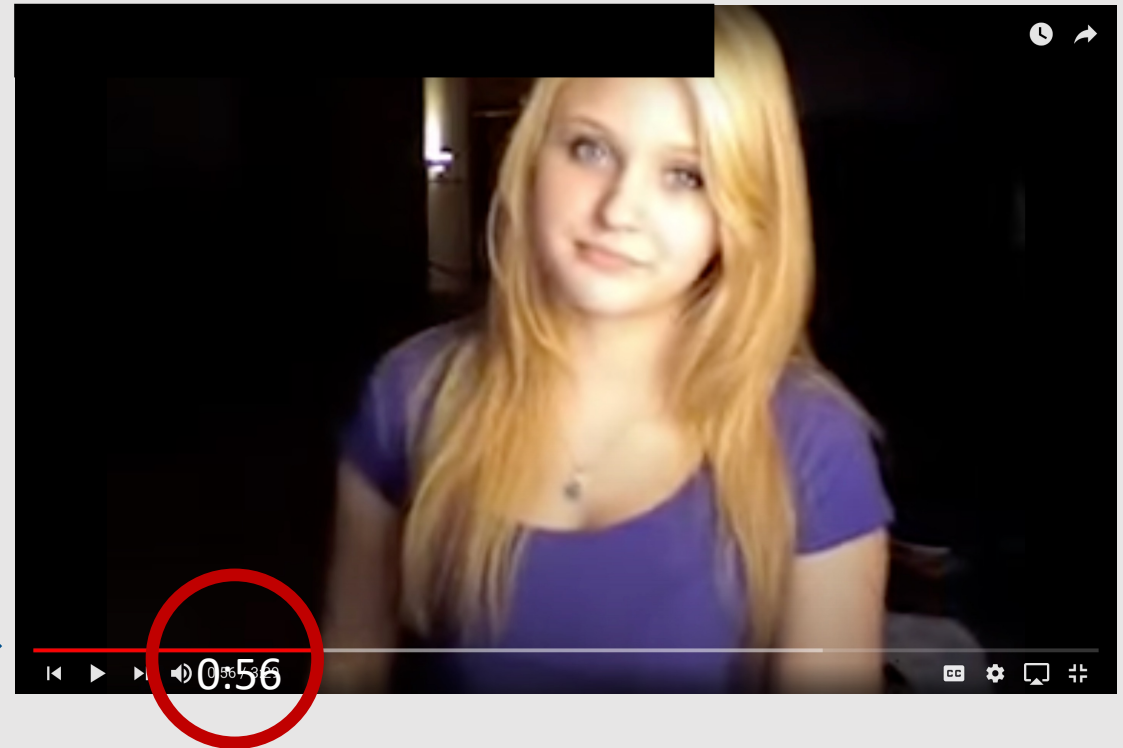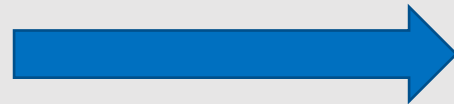
The Aftermath

- YouTube disabled comment sections for videos that appeared to be made by kids, for kids (exception for family Vloggers).

- It is easier to report and flag content.

- Advertisements are still posted on content created by minors.

Data Mining

- Data mining: (v) *the practice of analyzing large databases in order to generate new information.*

Responsible for your targeted ads and *unique/individualized* internet experience.

None of us see the <u>same</u> internet!

Individualized Internet

Everything you see online is tailored for you

- Every "free" platform or application you use isn't free.
- Data is the most valuable resource in the world—beating out oil and gold.
- Everyone sees the internet that is suited to their searches and views.

Internet wormholes

- Incel: (n) *"involuntary celibate";* a member of an online community of young men who consider themselves unable to attract women sexually, typically associated with views that are hostile toward women and men who are sexually active.

Free speech platforms and radicalization

- Reddit
- 4chan
- 8kun
- Parler
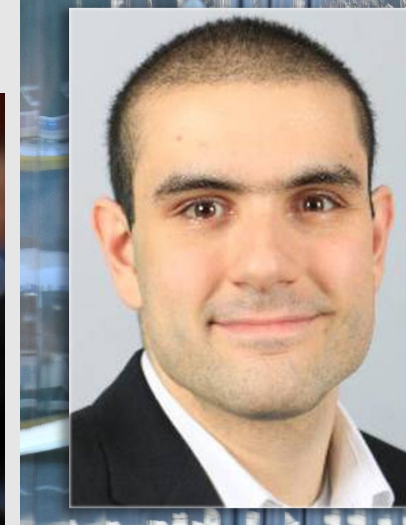
"You're canceled"

- Kyle Kashuv: Parkland shooting survivor had his Harvard acceptance letter rescinded after racist tweets and messages he engaged in at 16 were leaked by a 'former friend'.

- Billie Eilish: Videos resurfaced of the singer ranging in age from 13-17 making racial slurs, gestures, and appropriating black culture.

- Your online comments last forever.

Tweet

David Hill
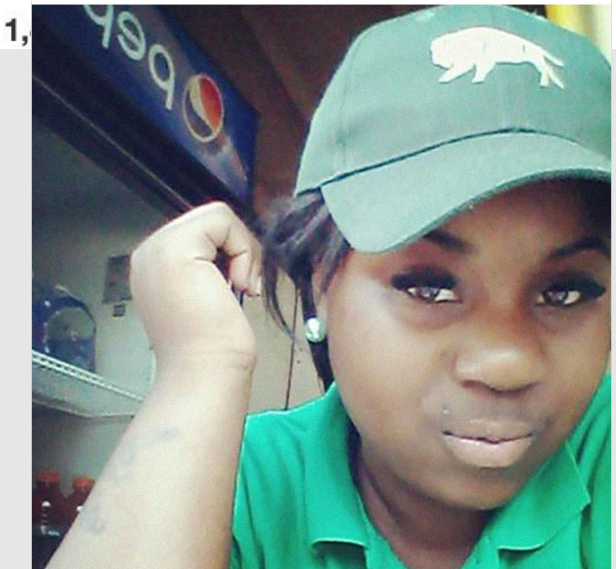@CoachDavidHill

We dropped a recruit this past week because of his twitter. We were ready to offer him until we saw some of the things he posted.

4/

at Brookfield Zoo

Wassup y'all?
At work serving these rude ass white people

1,

▶ **Kilroy's Downtown Indy**

I will never go back to this location for New Year's Eve!!! After the way we were treated when we spent $700+ and having our meal ruined by watching a dead person being wheeled out from an overdose my night has been ruined!!! Every year we have come to Kilroys to enjoy New Years Eve and tonight we were screamed at and had the manager walk away from use while we were trying to figure out our bill being messed up. The manager also told us someone dying was more important then us being there making us feel like our business didn't matter, but I guess allowing a Junkie in the building to overdose on your property is more important then paying customers who are spending a lot of money!! Our waitress when we were trying to ask about our bill being messed up also said "what do you want me to do [blur] pay your bill for you?" What a great way to talk to a paying customer! I get that working on New Years Eve is stressful but being a complete [blur] to us all night knowing you get an automatic gratuity is not right!!!

👍 Like   💬 Comment

Naomi 😎 H @NaomiH_official · 22h
EVERYONE SHUT THE [blur] UP

I GOT ACCEPTED FOR A NASA INTERNSHIP
💬 158   🔁 129   ♡ 3 447   ↑

Homer Hickam @HomerHickam · 3h
Language.
💬 1   🔁   ♡ 3   ↑

Naomi 😎 H @NaomiH_official · 2h
Suck my [blur] I'm working at NASA
💬 1   🔁 5   ♡ 65   ↑

Homer Hickam @HomerHickam · 2h
And I am on the National Space Council that oversees NASA.
💬 28   🔁 1   ♡ 3   ↑

You are not the worst thing you've ever done…

- "Canceling" is being weaponized to bully and embarrass minors.

- Children have greater rates of anxiety, depression, feelings of "otherness" than before the advent of social media.

- Parents: keep embarrassing posts about your children OFF the internet. Do not shame them for "likes".

Applications to be mindful of:

Considerations of:

- Privacy

- Bullying

- Psychological manipulation

- Child predators

Instagram

- An image sharing platform that allows users to share 15 second videos and photos (publicly or privately). Many people opt for the public option in order to gather a "following" and garner as many 'likes' as possible.

- Parents should know:
  - Photos are public by default.
  - Hashtags and location information can extend the reach of content posted beyond the user's followers unless privacy settings are changed.
  - *Sliding into those DMs*... Anyone can send a direct message to a user regardless of privacy settings. That being said, Instagram prohibits adults from DMing minors who they are not followers of. However, adults can DM minors who they *do* follow AND minors lie about their age.

TikTok

- A video sharing social network that mostly features teens dancing to popular music, singing, or engaging in viral "challenges".
- Parents should know:
  - Children and adults alike use the app. There are often creepy and sexually explicit comments about performers.
  - Swearing and sexual content is common. Challenges often feature "pranks" of a sexual nature (e.g. "me trying to kiss my best friend"; "watch me asking my friend if she 'wanna Bang'; "gray sweatpants challenge").
  - In 2019 the FTC imposed a record setting fine on TikTok's then parent company over illegally collecting information from children under the age of 13.
  - Kids seek out likes and followers by opting to have public profiles and engaging in viral trends.

Kik messenger

- With a goal of "connecting the world through chat", the app allows users to send text-based messages, photos, or videos.

- **Parents should know:**

  - Stranger danger: adults and children use the platform.

  - Several highly publicized cases involving older men pretending to be teens to solicit the nude photographs of minors and the murder of a 13 year old girl.

  - It's full of covert marketing--"promoted chats" are conversations between brands and users.

  - If you're curious about what your minor child is doing on KiK, ask them to show you the messages on their KiK account (note: logging into KiK on another device will delete chat history).

Snapchat

- A self-destructing text messaging and video app that allows users to set the length of time their posts are viewable.

- Parents should know:
    - "Self-destructing" does not mean the messages, pictures, or videos actually disappear. People can screen-capture content and save to their personal devices.
    - Kids are more likely to engage in risky behavior because of the illusion that a post doesn't have any permanence.
    - Features like "Snap Map" allow users from all over the world to watch public posts based on location.

Periscope

- A live streaming platform that enables users to click on uncensored live-streaming content from around the globe.

- **Parents should know:**
  - Stranger danger: adults and children use the platform and users can send private messages and comment live.
  - Users stream as a way of promoting Only-Fans accounts (fee based subscription to sexual content).
  - Age verification is easily overcome

Omegle

- A chat site that pairs strangers together in text chat or video chat. The pairing is anonymous but allows users to filter potential chat partners by shared interests.

- **Parents should know:**
  - STRANGER DANGER: users are paired with strangers and there is no registration required.
  - Omegle is filled with people looking for sexual chat and content. Parents should be extremely wary.

What can parents do?

- First and foremost, parents should be mindful of the content they choose to share online and in-person.

What can parents do?

- Set an example, limit access to your social media, and refrain from posting Information that might compromise your child's privacy. E.g. embarrassing photos, "shaming stories", or intimate details about your child's life.

- There is a trend emerging of successful suits being brought by children against their parents for sharing intimate photos.

What can parents do?

- Consider freezing your child's credit score.
  - Most people only consider their credit when they are in the market to buy a house or car. This makes minors easy targets of identity theft that can go unnoticed for prolonged periods.
    - Contact: Experian; Equifax, TransUnion

What can parents do?

- It's also important to be present and cognizant of your child's online activity. Use monitoring applications and limit accessibility.

Parental monitoring tools: Bark

- This application monitors texts, emails, and 30+ applications to detect and alert about questionable content that is indicative of violence, bullying, drugs and alcohol, suicide, and sex.

- Lowest annual cost: ~$100

Parental monitoring tools: Circle

- Circle is an application and network connected 'box' that intercepts traffic to limit and monitor device access. The application can track device locations, limit or prevent access to specific websites/applications or limit access by category (e.g. social media; violence; sexual content etc.).

- Lowest annual cost: ~$129

Parental monitoring tools: Mspy

- This application can be installed covertly. Parents should be mindful that the covert monitoring of your child's online activity is very likely to cause grievances if discovered.

- Parents should also know that secretly installing this application on the device of someone who is not your minor child (under the age of 18) is **illegal**. This app can screen capture and key-log. It monitors social media and captures incoming, outgoing, and deleted SMS messages. This app also allows parents to view photos sent or stored on devices.

- Lowest annual cost: ~$200

Parental monitoring tools: Qustodio

- This application limits games and time spent on apps while also blocking inappropriate content. It manages screen time, monitors activity on social media, blocks calls and can track your child's device on a map.

- Lowest annual cost: ~$60

Ending note

- Many of us grew up in a time where the internet was new, uncensored, Wild West territory (anyone remember *Rotten.com*?). Truth be told, it's worse now… but the tools parents can use have also improved exponentially.

- The most important thing you can do is to be aware—know what your kids are doing online and be mindful of your own actions on social media.