

# Children's Ad Tech and Privacy

Jacqueline Cooney  
Arnall Golden Gregory LLP

Amy Lawrence  
Chief Privacy Officer and Head of Legal,  
SuperAwesome



## Jacqueline Cooney

Partner, Co-Chair Privacy and Cybersecurity Practice  
Arnall Golden Gregory LLP  
[jacqueline.cooney@agg.com](mailto:jacqueline.cooney@agg.com)



## Amy Lawrence

Chief Privacy Officer and Head of Legal  
SuperAwesome  
[amy.lawrence@superawesome.com](mailto:amy.lawrence@superawesome.com)

# Children's Privacy – An Overview

What Do We Mean When We Talk About “Children”?

Why the Focus on Children's Privacy and Ad Tech in Recent Years?

Why Should All Companies Pay Attention to Changes in Children's Privacy and Ad Tech Laws?

- The term “child” or “minor” can mean different things in different jurisdictions.

<i>UN Convention on the Rights of the Child</i>	Human beings under 18
<i>COPPA</i>	Individuals under 13
<i>CCPA</i>	Consumers under 13 Consumers at least 13 and less than 16
<i>CA AADC</i>	Consumers under 18
<i>GDPR / GDPR-UK</i>	Children under 16 (member states may provide a lower ages, so long it is not below 13) Children under 13 in the United Kingdom
<i>UK AADC</i>	Children under 18

- Almost universally, under 13 is a “child” but 13-18 year olds’ data is often protected in some way
- Protections are different depending on what the law says
  - Some may have multiple categories (data use ok for certain age buckets, but not others)
  - Some countries protect up to age 21!

# Children's Privacy – An Overview

What Do We Mean When We Talk About “Children”?

Why the Focus on Children's Privacy and Ad Tech in Recent Years?

Why Should All Companies Pay Attention to Changes in Children's Privacy and Ad Tech Laws?

- As with many areas of privacy, both ad tech and children's data have been the focus of recent legislation and enforcements.
- Technology has advanced quickly as have the use cases for both marketing and children's data.
- AI has further complicated the landscape – the ability to gather, analyze, and generate data via AI tools and platforms has made it easy (and more complex) to use data collected online in more innovative ways.



# Children's Privacy – An Overview

What Do We Mean When We Talk About “Children”?

Why the Focus on Children's Privacy and Ad Tech in Recent Years?

Why Should All Companies Pay Attention to Changes in Children's Privacy and Ad Tech Laws?

- Just because a website or service is not directed at or marketed to children does not mean that children's data cannot be collected and used.
  - The adtech ecosystem uses the same information from all visitors, including:
    - Cookie data
    - Mobile identifiers (IDFA, Android ID)
    - Full IP
    - Lat/long
    - Browser information
- It is important for all companies engaged in data collection and online advertising to remain vigilant about the types of data they collect, how they use it, and whether they know (or should know) that children's data is part of their data sets.

## New privacy laws may hurt small businesses most

By Taylor Barkley  
Published May 4, 2024, 1:00 p.m. ET

 The Drum.

 NEW YORK POST

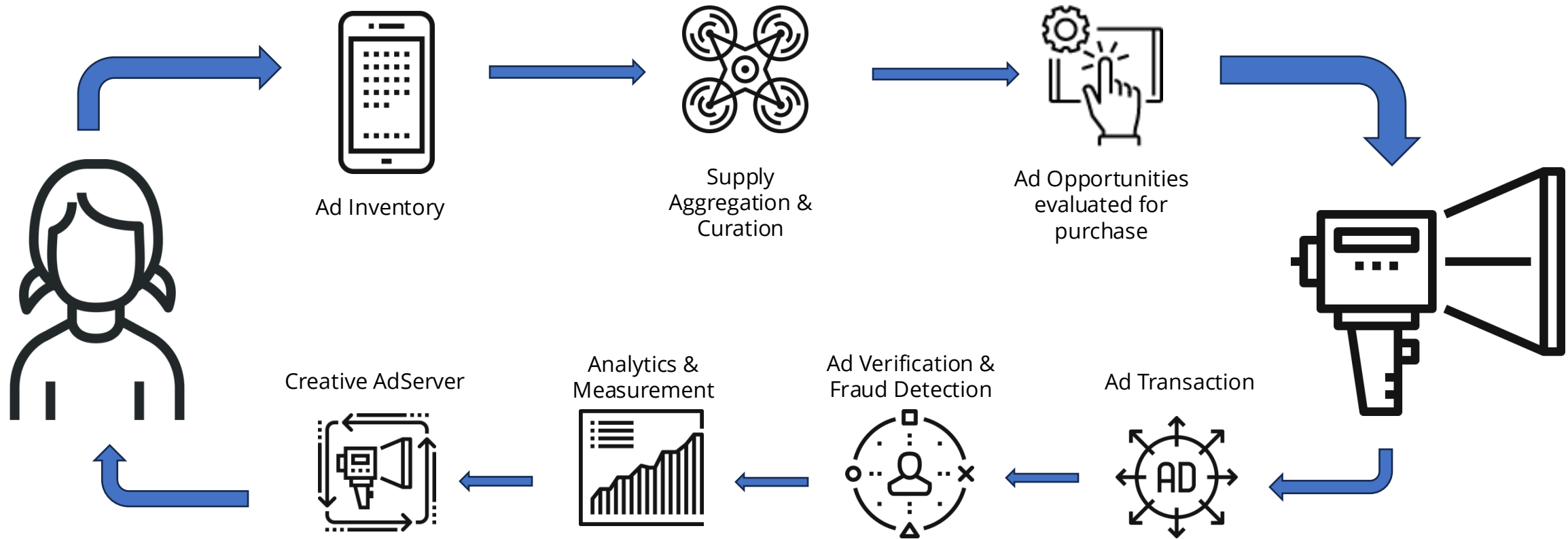
 adexchanger

## IAB rallies against FTC regulations that ‘could criminalize the internet itself’

DATA PRIVACY ROUNDUP

The FTC's PrivacyCon Was Chock-Full Of Warning Signs For Online Advertising

# Ad Tech – An Over-simplification



# Federal Laws and Legislation

## COPPA

- Applies to operators of websites or online services directed to children under 13
- Requires parental consent before collection of data of children under 13
  - UNLESS it is only used to provide support for specified internal operations
    - AND not used to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for **any other purpose**
- ^ This internal operations exception allows for contextual advertising to kids without parental consent

## Potential Changes to COPPA

- FTC proposed changes to COPPA in January, which (among other things):
  - Expands definition of personal information (including biometric data)
  - Allows for school authorization for collection and use of data by EdTech vendors
  - Requires separate parental consent for disclosures to 3<sup>rd</sup> parties
  - Permits text messages to obtain parental consent
  - Imposes specific security requirements related to sensitivity of children's data

## Pending Federal Legislation

- COPPA 2.0 and Kids Online Safety Act passed in the US Senate in July
- COPPA 2.0:
  - Expands COPPA protections to kids 13-16
  - Prohibits targeted advertising of u16s without consent
  - Requires compliance by companies even if they don't have "actual knowledge" of having kids' data
- KOSA
  - Creates duty of care for covered platforms
  - Requires default to most protective privacy settings
  - Allows users to limit or disable personalized algorithms and establishes other parental controls

# State Laws

## California

- **CCPA** – verifiable parental consent required for children under 13; consent for sale for children 14-16
- **CAADCA** – requires design changes for online services geared toward children under 18 (pending 1<sup>st</sup> Amendment challenge)

## Connecticut

- **CTPA** – requires opt in consent for children 13-15 for sale or targeted advertising; amendments require online services for children under 18 to design services to reduce risks to children

## Louisiana

- **SB 162** – prohibits social media companies from advertising to accounts of children under 16 based on the minor's personal information

## Maryland

- **MD AADC** – like CA AADC, but perhaps narrower applicability as it applies to services 'reasonably' likely to be accessed by children
- **MD ODPA** – prohibits targeted advertising and sale of data for children under 18 (all others have an opt out right)

## New York

- **CDPA** – for u13, permits processing as allowed under COPPA, but for 13-17 prohibits use of data for any marketing/advertising purposes

## Texas

- **HB 18 (SCOPE)** – prohibits social media companies from any advertising to accounts of children under 18 unless social media platform has parental approval

## Utah

- **SB 152** -- prohibits social media companies from any advertising to accounts of children under 18





## GDPR

- Children's data is treated as particularly sensitive
- Parental consent is required for collection of data for kids under 16
- EU countries can have a lower age (but not below 13)
- Online marketing in the EU already requires consent – parental consent potentially creates a “double” consent requirement

## UK Age-Appropriate Design Code

- 15 standards for online services (apps, games, connected toys/devices, new services)
- Requires:
  - mapping personal data collected from children
  - Checking age of people who visit website, download app, etc.
  - Switching off geolocation services
  - Not encouraging children to provide additional personal data

## Other EU Laws

- Digital Majority Law in France requires deactivation of social media accounts of under 15 unless parental consent
- Other EU countries have established lower ages for consent than required by GDPR, as well as additional restrictions on the use of certain types of children's data
- Other EU countries have implemented Age Appropriate Design Codes

## Federal Regulation

- The FTC has already brought enforcement actions under Section 5 alleging unfair and deceptive trade practices around the use of AI, including for the purposes of collecting and using children's data in AI platforms.
- The FTC's guidance "Self-Regulatory Principles for Online Advertising" has been interpreted to apply to AI generated content and advertisements.

## Self-Regulatory Schemes

- BBB's Children's Advertising Review Unit (CARU) Regulatory Guidelines for Children's Advertising provide guardrails for children's advertising.
- The guidelines require operators that use AI generated-content to ensure same safety guidelines used by advertisers when marketing products using real children.
- CARU Working Group developing additional guidelines for the use of AI in the kids space.

## Rules for Use of AI in Social Media

- AI generated content to market to children or to influence children's behavior and preferences should be used cautiously and ethically. AI should not be used to hide the intent or source of the messaging.
- The same online advertising rules should apply here, including transparency around any endorsements and use of AI generated content.
- The social media platform itself may have additional rules on use of AI.

# Using Ad Tech with Children in Mind

## Privacy Policy

- Update your privacy policy to ensure that you are making clear disclosures about what data you collect and how you use it.
- If you maintain a child-directed website, app, or game, make sure your policy is age-appropriate.

## Parental Consent

- Understand whether you need to seek parental consent when collecting data from children.
- Know the jurisdictions where you operate and follow local rules for ages of digital consent and other local obligations.

## Context-based Advertising

- Use context-based advertising for children instead of targeted or behavioral advertising.
- Avoid “stealth” or “blended” advertising in children’s games and apps where advertising is seamlessly meshed with the product.

## Consent-based Barriers to Content

- Make your content available without collecting personal data where possible so that consent is not required.
- Do not create unnecessary barriers to your content for the purposes of forcing consent (and therefore forcing the collection of personal data).

## Processes for obtaining consent

- Use clear, user-friendly means of obtaining parental consent.
- Ensure that your parental consent mechanisms don’t incentivize children to find ways to work around them.

**Thank you!**