Children’s Privacy Online: An Urgent Call to Action.

Ahmed Hani Yousef & Maria Belen Cuadros Carrion

Professor James Marquardt

Executive Summary

Problem & Context

Children are vulnerable, as they are in a developmental stage and therefore have fewer cognitive defenses and less awareness than adults. 95% of children have some access to the Internet. The average screen time of a teenager increased to 9 hours a day. Only 28% of parents feel confident teaching their child how to behave online. Simultaneously, rates of depression, eating disorders, and self-harm are increasing among children.

Root Causes & Causal Relationships

Companies use addictive & manipulative design techniques, such as Endless Scrolling, to drive up viewership. The techniques are successful, as 54% of children find it hard to give up social media, showing signs of dependence and addiction. Additionally, targeted algorithms have encouraged invasive data collection, resulting in the collection of an estimated 72 million data points on kids by the age of 13. The algorithms have shown to cause 'filter bubbles' and 'perfect storms' of inappropriate harmful content promoting drug use, eating disorders, and violence.

Status Quo & Implications

Children's Online Privacy Protection Act (1998), the current federal law is "hopelessly outdated" and "toothless", as over 80% of children falsify their age online. Multiple states have proposed and enacted their own children's privacy policies, likely creating a patchwork of laws that companies and individuals operating across state lines will have difficulties complying with. Inadvertently, causing children in states with less resources to receive inadequate protection.

Recommended Policy & Expected Outcomes:

The Age-Appropriate Design Code (AADC) is a comprehensive policy that ought to be used at the federal level, requiring online services to: put the interests of children first, minimize data collection, provide clear privacy policies, conduct a Data Protection Impact Assessment (DPIA), and set default privacy settings to highest.

Expected Benefits:

1. Increase the range of protection by defining children as consumers under the age of 18 instead of 13, since teenagers show different levels of maturity across that range.
2. Implementation of appropriate security measures that mitigate privacy risks associated with the processing of personal data, through conducting a DPIA.
3. Promote more responsible design practices through a Children's Data Protection Working Group, reducing reliance on addictive and manipulative techniques to make profit.

Expected Costs and Implementation Challenges:

1. Governmental investment required for enforcement, monitoring, and regular assessments of the policy.
2. Additional costs associated with business and service providers to implement the required changes.
3. Overcoming resistance from businesses, service providers, and lobbyists who may view the policy as overly restrictive or burdensome.

Key assumptions, risks, and success factors:

1. Assumptions include: Companies ability to develop the needed technology. Government ability to regulate and enforce the policy.
2. Risks include: Potential data breaches from DPIA (Cambridge Analytica), Overegulation might impact users experience, misinterpretation of guidelines.
3. Success factors: Education of parents and children on the updated policy, communication between the Working Group and the service providers.

Evaluation of Policy Effectiveness over time

The effectiveness can be evaluated using quantitative indicators such as: number of reported breaches, compliance rates, and number of children negatively affected by the Internet. Qualitative indicators include: user feedback, and evaluations of the policy impacts. Both need a regular assessment, to help update the policy and remain effective.

Understanding Internet Usage among Children

Children are Vulnerable

It is important to explain why this white paper emphasizes children's privacy rather than addressing privacy issues across all age groups. Children lack the ability to advocate for their own interests due to their age and cognitive capacity, necessitating our responsibility as a society and regulatory body to protect their privacy. This notion is commonly spoken by experts in the field. "The younger children are, the more vulnerable they are," says Dr Allen Kanner, a family and child psychologist (Post). Children also need to have the agency to choose who they want to become, without having algorithms predetermine and narrow down their future pathways. Shown in a research done by The Office of the Children's Commissioner, children do not have full understanding of the implications and future consequences of sharing their data compared to an adult (“Who Knows What About Me?"). Hence, this paper advances distinct protections for children’s privacy and wellbeing, to be carried out by parents, industries, governments, and society together.

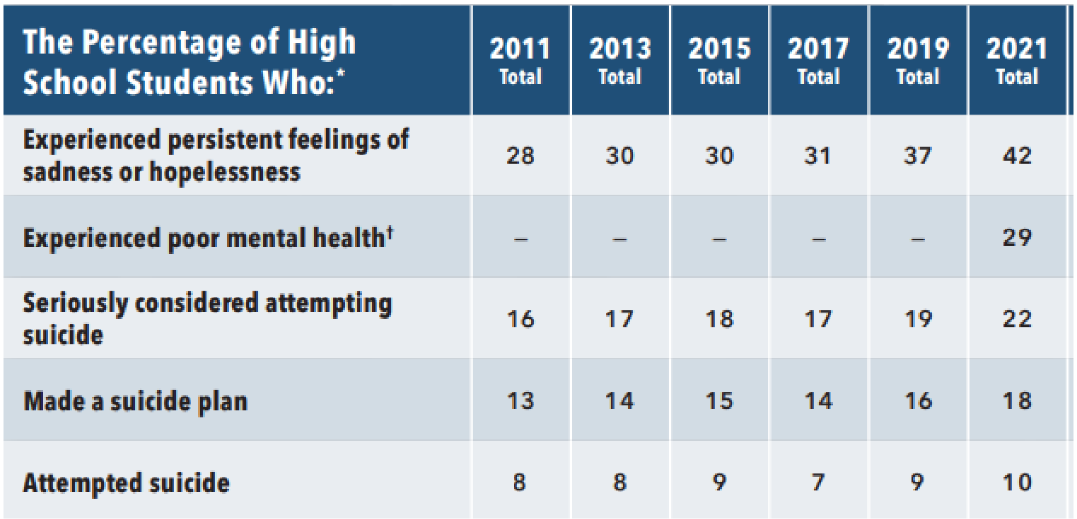
Spread of Internet

In a survey done by the *American Community Survey,* 95% of 3 to 18-year-olds had some access to the Internet in 2019 (“COE - Children’s Internet Access at Home”). This finding does not come off as a surprise, as the Internet is being integrated more into the everyday life of children. Accelerated by covid, children now use the Internet for socializing, gaming, and most recently, virtual learning, forcing parents and guardians to provide children some access to the Internet.

How do companies that provide Internet services free of charge monetize them and make profit? Similar to traditional radio channels, these service providers offer free content to users, which they then monetize by displaying advertisements for the highest bidder. Providers prioritize increasing viewership and engagement from their consumers by increasing the time spent on the website or application, and their efforts have been successful. While an increase of screen use is observed across all age groups, the most prominent rise has occurred among teenagers, as they spend an average of 9 hours on their screens -more than a third of their day. (American Academy of Child and Adolescent Psychiatry).

Alongside the growth in screen time, additional troubling trends have been detected among children and teenagers, including an increase in depression, self-harm, and eating disorders. The CDC's Youth Risk Behavior Survey Report showcases some of these trends, as seen in the following table.

(Source: CDC, Youth Risk Behavior Survey Data Summary & Trends Report, 2023)



The Percentage of High School Students Who:*	2011 Total	2013 Total	2015 Total	2017 Total	2019 Total	2021 Total
Experienced persistent feelings of sadness or hopelessness	28	30	30	31	37	42
Experienced poor mental health†	–	–	–	–	–	29
Seriously considered attempting suicide	16	17	18	17	19	22
Made a suicide plan	13	14	15	14	16	18
Attempted suicide	8	8	9	7	9	10

We maintain that the correlation between the crisis of children's mental health issues and excessive increase in screen time has two root causes: Addictive & Manipulative Design Techniques, and Targeted Algorithms.

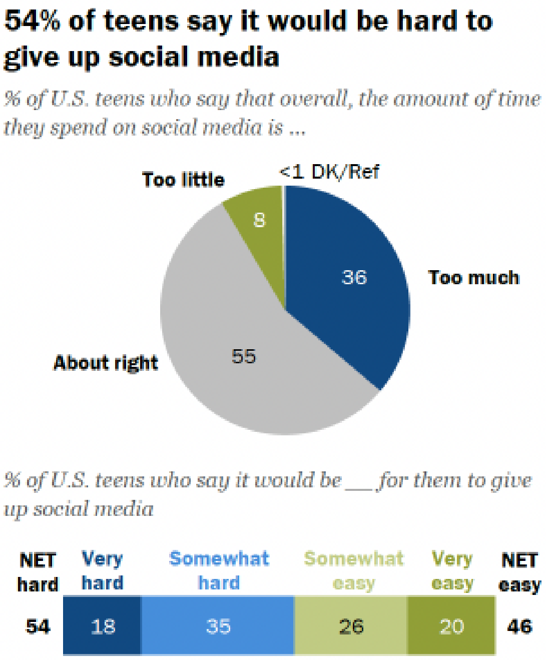
Addictive & Manipulative Design Techniques

Research by the Department of Psychology of the University of Notre Dame revealed that service providers employ a "vicious cycle involving user attention leading to powerful dopamine-related reinforcement, which then stimulates more attention intended to achieve more reinforcement"(Mujica et al.). Ex-employees of tech giants have spoken about exploiting the mentioned brain mechanism to manipulate people into using their services more often and for longer periods of time. "We took a page from Big Tobacco's playbook, working to make our offering addictive at the outset" said Tim Kendall, Facebook's former director of monetization (Holmes). Further research done by experts in psychology, game engineering, and algorithms have yielded the following results of psychological mechanisms that are designed to be manipulative and addictive (Montag et al.):

- **Endless scrolling /streaming:** A technique used to display more content infinitely without the user explicitly asking for it. Such as Youtube's AutoPlay, and Instagram's infinite feed.
- **Endowment effect**: As users go back to the service more often; They become emotionally attached, and it becomes harder for them to delete the application or stop revisiting the website.

- **Social Pressure:** Exerting pressure from peers to engage in the service more often, such as the blue ticks on Whatsapp.
- **Social Reward:** Known as the ‘like effect’, users seek validation and instant gratification through the number of likes, shares, and comments they receive on their posts.

These manipulative and addictive design techniques have proven to be quite effective, especially with children; A survey of American teenagers aged 13-17 done by Pew Research Center shows that while only 36% of teens think they spend too much time on social media, 54% think it would be either “very hard” or “somewhat hard” to give it up (Vogels et al.).



(Source: Teens, Social Media and Technology, Pew Research Center, 2022)

Increased Screen Time Impacts

The impacts of increased screen time on children are overwhelmingly negative, as leading experts in children psychology, neuroscience, and technology have expressed concerns on the matter. Jean Twenge, a psychology professor at San Diego State University, says “the more hours a teen uses social media, the more likely they will be depressed,” and the same goes for engaging in self harm (Kingson). These claims are backed up by studies done on the relationship between increased screen time, and effects on children's cognition: An NIH study of 12,000 participants aiming to understand media use impacts on a person's development has yielded preliminary results showing a correlation between screen use and premature thinning of the cerebral cortex (Paulus et al.) The cerebral cortex is the part of the brain responsible for the high-level processes, such as intelligence, personality, decision making, and memory.

Targeted Algorithms

The second root cause is targeted algorithms, which are data-driven computational processes that analyze users data and personal information to find trends and engagement patterns to deliver personalized content based on their interests, behavior, and demographics. The algorithms are designed to achieve a certain goal, which is typically to keep users engaged for longer periods of time. Success of the algorithm is heavily based on the quality and quantity of data it is fed, which is why more than 85% of websites use data trackers of some sort ("DuckDuckGo"). The popularity is due to how easy and lucrative it is for websites and applications to collect data on their users, from identifiers such as IP address and device id, to privacy information such as search and location history, which then can be used to infer race, ethnicity, interests, and more layered private information.

Children are a high-value target for the trackers, since they tend to share more information and are unaware of the privacy concerns raised by the data being collected on them. Research conducted by a

72 Million
Data points by the age of 13

London-Based firm with expertise in children's privacy showed that "by the time a child is 13, over 72 million pieces of personal data will have been captured about them" ("SuperAwesome").

Nature of Algorithms

Due to their nature, algorithms entail little to no human control. The design and development of the algorithm is done by a human, but most of the algorithms rely on machine learning, a process where the machine teaches itself without the interference of a human (Dionysios Demetis). A thorough investigation done by journals at the Wall Street Journal shows how corrupt the algorithms can be. Dozens of TikTok accounts were created using false identities with different locations, genders, and preferences, but all were minors (over 13 but under 18). The investigation showed that the algorithm suggested thousands of pieces of inappropriate content depicting sexual violence, glorification of drugs and eating disorders. Once the account starts liking and watching those videos, the algorithm reinforced that type of video to maximize screen time, disregarding their nature and their potential effects on the child (French).

Algorithms also result in the creation of "filter bubbles" where the content users see are based on the data collected about them, such as their previous click search histories, which in turn prevents users from encountering contradicting viewpoints or topics not of their usual like pattern (Rhodes).

Targeted Advertisements

Algorithms have found their way into advertisements, too. Instead of targeting audiences using only demographics such as location, advertising agencies resort to Behavioral Targeting. A technique where algorithms are able to track user's behavior and base their ads based on the previous data (Academy). Enabled by invasive data collection methods , advertisers have access to real-time data and feedback on their campaigns, such as view time of each individual user, if they hesitated before scrolling past the ad, or if they were quick to engage.

Targeted advertisements are specifically unethical when the target audience is children, as they are in their developmental stages and lack the ability to critically assess what they encounter online (Casey). Several studies have concurred that children under the age of 9 are cognitively incapable of recognizing the commercial purpose of advertising (Carter et al.). However, even until the age of 12, are incapable of understanding the ‘selling’ and ‘persuasive’ intent of advertisements.

Targeted advertisement Impacts on Children

A Task Force on Advertising and Children by the American Psychological Association conducted multiple studies and researches, and reported strong associations between increases in advertising for fast food and rates of childhood obesity, and a substantial relationship between children viewing ads of tobacco and alcohol ads and positive attitudes toward consuming such products (American Psychological Association). Studies have shown that increased advertisements also increase the sense of materialism in children, which is linked to scoring lower in UNICEF wellbeing index as well as having poorer academic performance (Garin).

The Status Quo

Currently the only federal law governing children's privacy in the United States is the *Children's Online Privacy Protection Act*, known as **COPPA**. Introduced in the Senate by Sen. Richard H. Bryan (D-Nevada) in 1998, signed into law by President Bill Clinton in the same year, and updated in 2013, the Act requires operators websites and apps that are directed towards children or that have actual knowledge that children are using their services to perform a number of responsibilities, notably:

- **Obtain** verifiable parental consent before the collection of information and data
- **Provide** parents with the ability to delete the collected data
- **Post** a clear and concise privacy policy
- **Implement** reasonable security measures to protect collected data
- **Dispose** data after the fulfillment of the purpose for which it was collected.

Enforcement

The enforcement of COPPA is overseen by the Federal Trade Commission **(FTC)**. The FTC has the authority to bring enforcement actions against operators who violate COPPA, and can seek civil penalties of up to $43,280 per violation. The FTC has also issued a set of guidelines for compliance with COPPA. The FTC has settled over 40 cases since COPPA was enacted, with a $170 million fine on Google and a $520 million fine on EPIC game company being their biggest cases (Privo).

Problems with COPPA

While providing some level of protection for children under the age of 13, COPPA has several shortcomings that have allowed companies to exploit children for profit. Firstly, COPPA is outdated and unable to keep up with the rapid pace of technological advancements. COPPA predates the invention of smartphones and social media platforms, which are now ubiquitous in the online experiences of children. Jim Steyer, founder and chief executive of Common Sense Media, has described COPPA as "hopelessly outdated" (Jargon). Another issue is that COPPA's protections are limited to children under 13, leaving older children and teenagers vulnerable to privacy violations and data breaches. In addition, COPPA only covers websites and apps that are directed towards children or that have actual knowledge that children are using their services. Since the seven approved methodologies for VPC are only a recommendation and not a requirement, most services resort to using a self-declaration checkbox that incentivizes them to not have knowledge of children's presence on their platforms ("Verifiable Parental Consent: The State of Play") resulting in children's data still being collected and used by companies that are not subject to COPPA. Self-declaration has been proven to be ineffective as research shows that over 80% of children lie about their age online to access such services (Sweny).

State Legislation

As COPPA has failed to adequately address the issue of children's online privacy and well-being, lawmakers at the state level have taken action to fill the gap. To date, two states have enacted their own children's privacy laws.

In 2022, California passed the first-of-its-kind bipartisan Age-Appropriate Design Code Act, which was introduced by California State Assembly members Buffy Wicks (D) and Jordan Cunningham (R). The law takes a privacy-by-design approach, requiring companies to prioritize the privacy and well-being of children throughout the design process, by setting default privacy settings to the highest, minimizing data collected on children, and other policy elements. This approach has been adopted by other states, including Maryland, Minnesota, Nevada, and New Mexico, which have introduced similar laws in response.

On March 23, 2023, Utah's Governor Spencer Cox, signed two Senate Bills 152, and 311, which take a more regulatory approach. The bills were introduced in Utah's state legislature by Rep. Brady Brammer (R), and the laws will go into effect on January 1, 2024.

The bill requires social media platforms to:

- **Verify** the age of all users, and require Parental Consent for children;
- **Give** parents full access to their children's accounts;
- **Create** a default curfew setting that blocks access overnight;
- **Ban** data collection and targeted algorithms.

The efforts of state legislators to address the issue of children's privacy are certainly well-intended, but the state legislation carries unintended consequences. With each state proposing its own policy for children's privacy, the result will be a patchwork of potentially 50 different laws that will create confusion and compliance problems for companies and individuals operating across state lines, thus likely producing costly litigation.

Also, some of the bills (both passed and proposed), have been met with heavy criticism from both civil rights groups and tech industry representatives. According to Ari Cohn, a lawyer for TechFreedom, the new bills passed in Utah violate the First Amendment's right to free speech and pose a threat to the Internet's integrity (Alberty). The TechFreedom letter also notes that the Supreme Court has previously invalidated less sweeping laws in the past three decades that restrict minors' access to speech via social media. Moreover, the requirement for social media companies to obtain parental consent has also been criticized as a potential cause for exclusion, particularly for marginalized children whose parents may not be willing or able to give consent (Singh). Finally, not all states have the same resources to be dedicated for the enforcement and implementation of children’s privacy laws. A potential outcome is children in states with lower resources having less privacy and protection than those in more wealthy states.

Therefore, a federal policy option must be proposed to protect children's privacy across the nation, while balancing the benefits of advancing technology. Each policy option should be thoroughly explored, including benefit-cost analysis and tradeoffs to determine the best solution.

Policy Options

Public Awareness and Educational Campaigns

72%
OF PARENTS ARE NOT EDUCATED ENOUGH ON CHILDREN PRIVACY ISSUES

According to a 2020 survey by Pew Research Center, only 28% of parents say they are very confident in their ability to teach their child how to behave online safely and responsibly (Auxier et al.). A similar study the Reboot Foundation found that while many children today may be considered "digital natives," they lack critical digital literacy skills, including the ability to distinguish between credible and fake online information (Strauss).

Raising awareness through educational campaigns is a policy option designed to promote responsible digital citizenship among children and young people. This solution emphasizes the importance of fostering digital literacy skills and critical thinking among children, while parents are informed on how to monitor their children's online activity and set healthy boundaries. By doing so, children will be able to identify potential dangers online, avoid risky behavior, and seek help when necessary.

A potential implementation of this solution is to develop a curriculum for students that can be given at different milestones in schools, this has been done before and can be modeled after **Common Sense's Digital Citizenship Curriculum**. Over a million teachers use their curriculum worldwide, and according to a national survey of teachers. Specifically 69% of teachers reported that their students were more knowledgeable about how to protect their online privacy (Carrie et al.).

The solution would result in beneficial long-term effects on both children and parents, as this will help individuals protect themselves even if the service providers do not have their wellbeing as a priority. Additionally, the nature of the solution requires minimal regulation from the government, and would have low monetary costs compared to more technical solutions. Similar efforts have been made in the context of tobacco use by children. For example, the "Truth" campaign launched by the American Legacy Foundation in 2000 aimed to raise awareness about the harmful effects of smoking and the manipulative tactics used by the tobacco industry. It resulted in keeping over 450,000 teenagers from starting to smoke and saved over $2 billion in health costs in its first 4 years (“Truth Campaign”).

While the policy can be effective, there are also potential drawbacks to consider. Firstly, these campaigns may not be accessible to all children due to a lack of resources and funding, leaving marginalized communities at a disadvantage (Smedley et al.). Moreover, the solution may take time to have an impact, the curriculum would require frequent updates to maintain pace with advancing technologies, resulting in significant maintenance costs. Finally, service providers may still use addictive and manipulative design techniques that can undermine the effectiveness of educational campaigns.

This policy option offers a promising long-term approach to promoting safe and responsible online behavior. However, it does not address systemic privacy concerns like unconsented data collection and targeted content and advertisements. Nonetheless, it is an important step towards long-term policy solutions.

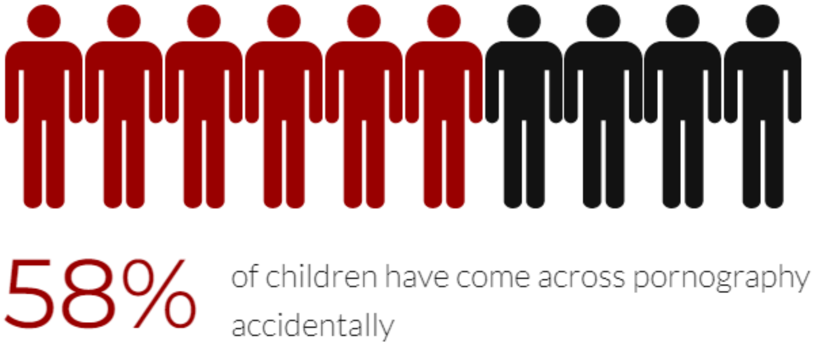
Age verification

Age verification as a policy option seeks to prevent children from accessing services that might contain inappropriate content, through the process of verifying each user's age before getting access to the service. Age-restricted content ranges from pornography to harmful content such as videos promoting drug use or eating disorders. By its nature, this solution would require every person to verify their age to distinguish between children and adults.

The mechanism of implementation has been a topic of discussion for years, and a recent example would be Loiusiana's Act no. 142, requiring age verification for accessing pornographic websites. The Bill was introduced by Rep. Mark Wright (R) in 2022, passed by the Louisiana State Legislature, signed into law by Governor John Bel Edwards (D) on May 23, and went into effect on January 1, 2023 . The bill requires commercial pornography websites to implement age verification systems that prevent access to users who are under the age of 18. To comply with the law, commercial pornography websites must either use a third-party age verification service or implement their own system. Websites that fail to comply with the law can be fined up to $10,000 per violation.

A similar solution can be implemented with a wider range of services, such as social media platforms, which have proven to promote inappropriate content for children resulting in increased screen time and worsening wellbeing. The solution would benefit children by preventing them from accessing content that might be harmful for them. A survey by

CommonSense Media in 2022 showed that 58% of children have come across pornography accidentally (Robb). Additionally, age verification can help enforce data collection regulations that are being ignored by websites benefiting from not having ‘actual knowledge’ of children among their users .



However, the solution has several potential costs and drawbacks that must be considered. Firstly, implementing age verification mechanisms or seeking third-party tools is an added cost that could be challenging for smaller platforms. Additionally, an unintended consequence of the policy would be children resorting to alternative ways to access the content, such as Fake IDs. Another potential drawback is the potential use for censorship, raising constitutional issues as seen with Utah’s law, with free speech lawyers such as Ari Cohn observing that the bills would "violate the First Amendment and threaten to fragment the Internet" (Habeshian). Finally, the policy would require individuals to provide personal information, such as IDs, which could lead to privacy and security risks. Hackers could potentially gain access to this information and use it for nefarious purposes, such as identity theft. According to a study done by Javelin Strategy, in 2017 more than one million children were victims of identity fraud, with the digital world being the main area of occurrence (Pascaul and Marchini).

Age verification is a complex policy option that requires a balance between privacy protection and potential tradeoffs. While it can help mitigate the risks of children being exposed to inappropriate content and enhance their online privacy and security, it may come at the expense of free speech and the unintended consequences of children seeking alternative ways to access inappropriate content.

Banning targeted algorithms

Banning targeted algorithms for minors is a policy option that seeks to protect children's privacy and prevent the manipulation of their behavior by service providers and advertisers. This policy option would prohibit the use of algorithms that are designed to target children for advertising, content recommendations, or other purposes. By doing so, children will be less likely to be exposed to inappropriate content with the goal of increasing their screen time, as well as prevent the manipulation done by targeted advertisement that exploits the vulnerability of children.

Previously proposed legislation has explored the possibility of such a solution, such as the Minnesota House File 3724 introduced by Rep. Peter Fischer (D) in 2022. If enacted, the bill would require social media platforms to provide users under the age of 18 with the option to disable algorithmic recommendations and suggestions. By implementing this policy, companies would have to rely on more general advertising based on context instead of engagement and behavior. The platforms would also have to establish procedures to verify the age of users and disable the use of algorithms for users who identify as minors .

The solution brings a multitude of benefits for children, as the ban of targeted algorithms will force companies to rely on contextual advertisement which is more general and less invasive than behavior based one. By doing so, manipulation of children for profits by advertising agencies and political actors will be reduced, giving children more agency and freedom to choose who they want to be. Additionally, targeted content is one of the main techniques service providers are exploiting children's dopamine cycles by re-enforcing them to give attention to feel happy and satisfied. By banning it completely, this would restore some balance to how children experience joy and happiness, making it less addictive. Finally, previously mentioned phenomena of 'echo chambers' and 'filter bubbles' will be immensely reduced by giving children content that is not based on what they would like the most, and instead views from different perspectives and ideologies.

While banning targeted algorithms for minors may seem like a good solution to prevent exposure to harmful content, it has some potential drawbacks. Firstly, the ban could negatively impact smaller websites that rely heavily on ad revenue. These sites would lose out on the ability to target ads to specific users based on their interests and behaviors, resulting in a loss of revenue, as well as a decline in the quality of advertisements. However, there are concerns that the ban could violate the First Amendment, as it may be seen as a restriction on commercial speech. In a case related to a similar law in Vermont, a judge ruled that "targeted ads are a form of protected speech" (Brodkin). Therefore, a ban on targeted algorithms for minors would most certainly face successful legal challenges. Finally, algorithms are not all used with malicious intent, as sorting done by search engines, for example, helps researchers find information easier and more efficiently, which would also have to be limited due to the broad definition a policy like this would entail.

Banning targeted algorithms for minors is a potentially effective policy option that seeks to protect children's privacy and prevent manipulation. However, it may negatively impact smaller websites reliant on ad revenue, face legal and constitutional challenges, and limit the potential for useful algorithms. Despite the concerns raised, banning targeted algorithms for minors is an important policy option that should be thoroughly examined for its potential benefits and drawbacks.

Proposed Policy

Age-Appropriate Design Code (AADC)

While most policy options aim to regulate how children's data is used online, the complexity of the problem and its underlying causes requires a more comprehensive solution, one that fundamentally addresses the way children experience a digital world that was not designed with their best interests in mind. The Age-Appropriate Design Code (AADC) developed in the United Kingdom in 2019, and adopted in California in 2022, is a forward-thinking policy that addresses the need to protect children's privacy not from the Internet, but within it. The code consists of a set of guidelines and standards that covered entities must follow to ensure the unique needs and vulnerabilities of children are met throughout the entire lifecycle of the product or service. While we used the enacted California Bill as a model, we acknowledge the need to implement modifications to some elements to address certain limitations, and for the policy to be more manageable at the federal level.

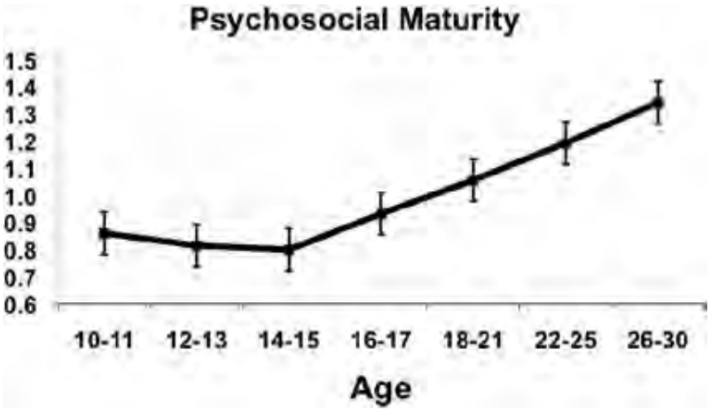
The Core Elements of the AADC

- Increase the coverage to include services likely to be accessed by children under 18.
- Require covered entities to implement a privacy by design approach that takes the children's best interests in consideration.
- Require covered entities to balance the confidence of age estimation appropriately to the risks arising from the data practices
- Require covered entities to conduct a Data Protection Impact Assessment (DPIA) before releasing a feature to the public.
- Require covered entities to provide concise, clear, and easy to understand privacy policies
- Establish a Data Protection Working Group tasked with recommending best practices, and providing implementation guidance for covered entities.

Covered Entities & Scope

Children are defined as consumers under 18 years of age for the AADC which differs from COPPA (age 13). This change recognizes that older children might not have the same level of maturity or decision-making capacity as adults, making them more vulnerable to online harms and privacy violations. This is supported by different researchers, such as the American Psychological Association and its research on the maturity of adolescents.

Figure 1
Psychosocial Maturity (Standardized Composite Scores) as a Function of Age (in Years)



(Source: American Psychologist, 2009)

As we can see significant differences were found between 16-17 year olds and those 22 and older, and between 18-21 year olds and those 26 and older. So, we can conclude that increasing the range protects children under 18, because they are also a vulnerable group.

COPPA applies to firms that have actual knowledge of the collection of personal information from children. This may incentivize ignorance as over 80% of children lie about their age on social media. In contrast, the AADC does not mention actual knowledge but focuses on the likelihood of children accessing the online service, product, or feature based on indicators such as; a significant amount of the audience is determined to be children, the platforms have design elements known to be interest of children, the content are directed to children.

Privacy By Design

Covered entities must prioritize children's well-being and privacy throughout the entire lifecycle of their products or services, beginning with the design phase. The (AADC) establishes a set of standards and practices that must be implemented, such as setting default privacy settings to the 'highest level'. Since most children tend to accept preselected options, covered entities need to ensure that privacy settings for personal data not essential for the core service are set to 'do not share', unless the child decides otherwise.

AADC also mandates that entities enhance their data management practices by limiting data collection from children to only what is absolutely necessary for providing the core service and deleting the data once its intended purpose has been served. Entities are prohibited from sharing children's data with third parties unless it is demonstrated that such sharing is necessary for the service's operation.

Lastly, entities are prohibited from using children's data in ways that could be detrimental to their well-being. This can be achieved by staying informed about industry standards and practices, as well as any research findings on harmful data usage. For instance, profiling children for targeted marketing purposes has been shown to negatively impact their mental health.

Risk-Based Age Estimation

While the AADC expands the age range to include children under 18, this alone does not resolve the issue of determining a user's age. Self-declaration methods have proven to be insufficient, while age-verification methods pose greater privacy risks when implemented across all covered services. Consequently, the AADC requires companies to establish users' ages with a level of certainty appropriate to the risks posed by processing children’s personal data, or to provide heightened privacy protections for all users.

The risk-based approach grants covered entities flexibility in selecting age estimation methods, but these must be proportionate to the potential harms to children resulting from the service in question. After assessing the risks to children that may arise from personal data processing, a confidence level must be met to ensure that if the user is a child, specific protections are implemented. Self-declaration may suffice for low-risk situations, while artificial intelligence or age-verification services might be necessary for higher-risk cases.

The AADC considers the inherent risk of age estimation, which involves collecting and processing more user data. That is why companies would be prohibited from using data gathered for age estimation purposes for other reasons. Lastly, while the California AADC requires companies to consider five different age groups for children, we recognize that this may be challenging for companies to implement initially and could pose an implementation obstacle. Therefore, we suggest simplifying the approach by defining a child as a consumer under the age of 18.

The Role of DPIA under the ADCA

The AADC requires covered entities to conduct a Data Protection Impact Assessment (DPIA). DPIA refers to a system created to identify risks related to the processing of personal data and to take measures to reduce them. There are key elements for processes such as; identifying the need for a DPIA, describing the processing, considering consultation, among others. However, under California Code there are problems with the DPIA system, such as potential ineffectiveness due to lack of experience or knowledge in data privacy, and inadequate follow-up on privacy risks. For example, in the Cambridge Analytica case, Facebook conducted a DPIA but did not properly react to the results, leading to a privacy violation and subsequent fine of 5 billion dollars. Despite being a relatively new system implemented in 2018, these issues can be addressed through training and development initiatives for staff conducting DPIAs, including instruction on privacy laws, threat assessment methods, and best practices.

Under our proposal, organizations must ensure they have a clear mechanism for following up on the results and suggestions of the DPIA to address the issue of insufficient measures to limit privacy risks. This may involve establishing a time limit for putting any required updates or modifications into action, appointing someone to monitor the implementation procedure, and carrying out routine evaluations to make sure the privacy concerns have been adequately reduced. Nevertheless, it is important to notice that this would be a long-term solution.

Transparency Requirement

Under the AADC, firms are subject to a Transparency Requirement. This means that organizations must have concise, clear, and easy-to-understand policies regarding their data collection. It also requires organizations to provide parents with the option to review and delete the information collected about their children, giving parents better access to the data collected about their kids. Lastly, this information and options must be presented in an easy-to-access way and should be displayed prominently.

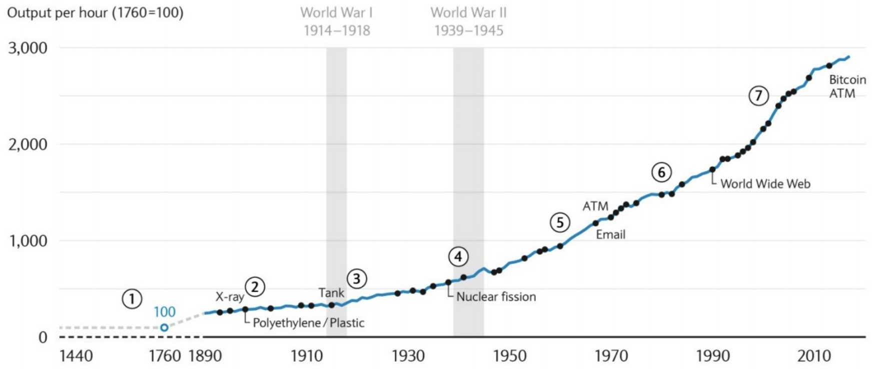
One way for organizations to comply with the AADC transparency requirement is by providing all privacy notices in clear language that children can understand, taking into consideration age groups. This promotes children's awareness of their privacy rights and prevents unintended data collection. However, measuring effectiveness may be challenging due to varying language abilities of different age groups and costly. Children's language under 18 varies according to their age. Children between 4- and 7-years old use simpler sentences and less complex vocabulary compared to those between the ages of 8 and 11, and the same pattern applies to teenagers and younger children (Pediatrics in Review, 2019). That is why we proposed using a neutral and easy language that even children under 13 can understand, as older children would still comprehend it. Utilizing a unified language for privacy notices would be more effective than designing specific language for different age groups and reduce the cost for such designs.

The Children's Data Protection Working Group

The AADC establishes the Children's Data Protection Working Group to develop privacy guidelines, standards, and information for protecting children's online privacy. The group's responsibilities include identifying online features and services commonly used by children and creating age verification procedures to reduce online risks. The group also addresses terminology in privacy regulations and policies that are easy for kids to understand. However, under California Code only 10 people from this state carry out this process which leads to greater challenges for them to catch up with the complexity of legislation, rapid technological development, and potential impact on innovation and internet services for children may need to be addressed.

FIGURE 1

From the printing press to the global internet, technology has evolved, and human societies with it



(Source: How technology has changed the world to work, World Economic Forum, 2018)

At a federal level the Working Group would consist of more than 10 people from different states if possible at least one of each of them with expertises on technological, educational, privacy, psychological fields, among others. Also, establishing a process for regular reviews and updates of regulations is one way to overcome the potential drawback of the California Children's Data Protection Working Group being too slow to catch up with fast evolving technology. This can include setting a schedule for regular evaluations of the laws and rules to make sure they continue to be applicable and efficient in safeguarding children's online privacy in the face of developing technology.

The Children's Data Protection Working Group might not have the resources necessary to update rules and regulations since it could take a long time. However, it is important to apply this proposed solution regularly so the Working Group can catch up with fast evolving technology at a similar rate.

Enforcement of AADC

Violations to the California Age-Appropriate Design Code Act (ADCA) detected by the working group would be fined. The fine is dependent on how many children are affected by the violation of terms and varies depending on whether it was intentional or a matter of negligence. Intentional fines cost $7,500 USD per child, while unintentional fines cost $2,500 USD per child. The purpose of the law is to establish the magnitude of penalties in case of violations and hold companies and organizations accountable for any harm caused to minors. This will ensure that online platforms prioritize the safety and privacy of children, promoting responsible behavior in the industry.

The standardized fines established by the ADCA may not fully account for the varying levels of harm caused by different violations to children. While the fines serve as a deterrent and promote compliance with the law, they may not be adequate to address the more severe harm caused by some violations. Moreover, the standardized fines do not consider the size or financial capacity of the organization or company responsible for the violation. The policy may be effective in protecting children from websites where the creator company cannot afford to pay the fines, but large corporations may be willing to challenge the law and even violate the policy to some extent if it is profitable for them. Therefore, it may be necessary to explore alternative approaches to enforce the ADCA, such as imposing more flexible fines that take into account the severity of the violation and the financial capacity of the organization.

Policy Evaluation

Key Assumptions

One key assumption for implementing AADC as a federal law is that the government has the necessary technology infrastructure, and resources for national level enforcement. This includes enforcing privacy settings, verifying compliance with design standards and conducting audits. It also assumes the government's ability to adapt and evolve its technology capabilities over time.

Risks & Unintended Consequences

A risk associated with the Working Group is potential misinterpretation of their guidelines and standards. Despite companies' well-intended actions towards compliance, there may be a risk of misunderstanding or misinterpretation of the recommendations, leading to failure in full compliance. Failure to comply with the regulations or guidelines set by the Working Group could result in penalties ranging from $2.2 million to $39.22 million (Globalscape).

A potential unintended consequence of conducting a Data Protection Impact Assessment (DPIA) is increased data breach risk. During the DPIA process, when sensitive data is collected and analyzed, data breaches may occur if proper security measures are not in place. This could lead to unauthorized access and potential harm to individuals and organizations, as exemplified by the Cambridge Analytica issue.

Complying with the AADC as a federal law may impact user experience. Changes to design or content, or to meet regulations could affect usability, functionality, and enjoyment for all users. These restrictions on age-inappropriate content may result in limitations or modifications to the user experience, potentially affecting satisfaction, engagement, and retention. Balancing design elements to adhere to the AADC may require careful consideration to maintain a positive user experience.

Implementation challenges & barriers

Implementing this policy as a federal law presents challenges for businesses, especially small enterprises, due to financial costs associated with compliance. Changes to data collection practices, consent mechanisms, and privacy policies may be required, along with potential impacts on business processes, resource allocation, and revenue streams. Ensuring compliance without disproportionate burdens may require careful planning and support mechanisms.

Implementing the Age-Appropriate Design Code as a federal law may face challenges due to legal and regulatory complexities. This includes interpretation and alignment with existing privacy laws, coordination with stakeholders, and potential conflicts with other regulations. For instance, there may be discrepancies between the Age-Appropriate Design Code's age definition (under 18) and other laws like COPPA (under 13). Complying with diverse requirements and aligning with other laws can complicate the implementation process. Careful consideration and addressing of these challenges may be necessary for effective implementation of the Age-Appropriate Design Code as a federal law.

A potential challenge implication of age-appropriate design code as a federal law could be legal pushback from service providers resisting the policy to protect their profits. This may involve challenging regulations, seeking exemptions, or pushing for changes that could weaken or delay implementation. Such legal challenges could create obstacles and delays in enforcing the policy, potentially impacting the intended outcomes of protecting children's well-being and online safety.

Success Factors

Successful implementation of age-appropriate design code as a federal law relies on collaboration and compliance among developers, service providers, and stakeholders. It assumes effective enforcement mechanisms, such as penalties or fines, for non-compliance. Collaboration is crucial for aligning digital products and services with design standards, and compliance is essential for protecting children online.

Moving forward with the AADC

Upon the implementation of the policy, an evaluation strategy is essential to assess and track its effectiveness and implications, particularly in the face of rapid technological advancements and ever-changing trends. The policy's success can be measured through quantitative indicators, such as a decline in mental health issues among children, and an improvement in their overall well-being and privacy. Qualitative indicators, on the other hand, encompass annual reports from the Working Group, as well as feedback from parents and children themselves.

A continuous review and adjustment of the key performance indicators is necessary to ensure a thorough evaluation, taking into account recent advances and shifting trends in the online environment to. This continuous assessment can point up areas for enhancement and make sure the policy continues to be effective in defending children's online rights and safety.

As technology continues to intertwine with every aspect of our lives, the urgency of protecting children's online privacy cannot be overstated. The Age-Appropriate Design Code presents a novel approach that targets the very foundation of the Internet and tackles the problem at its roots.While corporations reap enormous profits, more and more children are suffering from depression and attempting to take their own lives. If we hesitate to implement safeguards for children's privacy, then we are essentially surrendering our children's wellbeing and future to those who seek to exploit it for profits.

Works Cited:

Academy, Tutort. “Data Science for Targeted Advertising.” *Medium*, 5 Jan. 2022, www.google.com/url?q=medium.com/@-TutortAcademy/data-science-for-targeted-advertising-1ce5dc8060b7&sa=D&source=docs&ust=1681056023380742&usg=AOvVaw1AfVpParLf-quc4y-FXyym.

Alberty, Erin. “Utah Governor Twitter-Fights Free Speech Lawyer.” *Axios*, 17 Mar. 2023, www.axios.com/local/salt-lake-city/2023/03/17/utah-governor-cox-social-media-fight-twitter-techfreedom-kids.

American Academy of Child and Adolescent Psychiatry. “Screen Time and Children.” *Aacap.org*, American Academy of Child and Adolescent Psychiatry, Feb. 2020, www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-And-Watching-TV-054.aspx.

American Psychological Association. “Report of the APA Task Force on Advertising and Children.” *Apa.org*, 2004, www.apa.org/pubs/reports/advertising-children.

Auxier, Brooke, et al. “Parents’ Attitudes – and Experiences – Related to Digital Technology.” *Pew Research Center: Internet, Science & Tech*, 28 July 2020, www.pewresearch.org/internet/2020/07/28/parents-attitudes-and-experiences-related-to-digital-technology/.

Brodkin, Jon. “Proposed Law in Minnesota Would Ban Algorithms to Protect the Children.” *Ars Technica*, 18 Mar. 2022, arstechnica.com/tech-policy/2022/03/proposed-law-in-minnesota-would-ban-algorithms-to-protect-the-children/.

Carter, Owen B.J., et al. “Children’s Understanding of the Selling versus Persuasive Intent of Junk Food Advertising: Implications for Regulation.” *Social Science & Medicine*, vol. 72, no. 6, Mar. 2011, pp. 962–968, https://doi.org/10.1016/j.socscimed.2011.01.018.

“COE - Children’s Internet Access at Home.” *Nces.ed.gov*, May 2021, nces.ed.gov/programs/coe/indicator/cch/home-internet-access.

Dionysios Demetis. “Algorithms Have Already Taken over Human Decision Making.” *The Conversation*, 8 Mar. 2019, theconversation.com/algorithms-have-already-taken-over-human-decision-making-111436.

“DuckDuckGo Tracker Radar Exposes Hidden Tracking.” *DuckDuckGo Blog*, 5 Mar. 2020, spreadprivacy.com/duckduckgo-tracker-radar/.

French, Rob Barry, Georgia Wells, John West, Joanna Stern and Jason. “How TikTok Serves up Sex and Drug Videos to Minors.” *Wall Street Journal*, 8 Sept. 2021, www.wsj.com/articles/tiktok-algorithm-sex-drugs-minors-11631052944.

Garin, Sam. “Marketing and Materialism.” *Fairplay*, Oct. 2019, fairplayforkids.org/pf/marketing-and-materialism/.

Habeshian, Sareen. “Utah Becomes First State to Sign Law Limiting Kids’ Social Media Use.” *Axios*, 24 Mar. 2023, www.axios.com/2023/03/24/utah-limit-kids-social-media.

Holmes, Aaron. “Facebook’s Former Director of Monetization Says Facebook Intentionally Made Its Product as Addictive as Cigarettes — and Now He Fears It Could Cause “Civil War.”” *Business Insider*, 24 Sept. 2020, www.businessinsider.com/former-facebook-exec-addictive-as-cigarettes-tim-kendall-2020-9.

Jargon, Julie. “How 13 Became the Internet’s Age of Adulthood.” *Wall Street Journal*, 18 June 2019, www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201.

Kingson, Jennifer A. “Social Media’s Effects on Teen Mental Health Comes into Focus.” *Axios*, 11 Jan. 2023, www.axios.com/2023/01/11/social-media-children-teenagers-mental-health-tiktok-meta-facebook-snapchat.

“Legacy’s Truth Campaign Named One of the Top Ad Campaigns of the 21st….” *Campaign for Tobacco-Free Kids*, 14 Jan. 2015, tobaccofreekids.org/blog/2015_01_14_legacy.

Montag, Christian, et al. “Addictive Features of Social Media/Messenger Platforms and Freemium Games against the Background of Psychological and Economic Theories.” *International Journal of Environmental Research and Public Health*, vol. 16, no. 14, 23 July 2019, p. 2612, www.mdpi.com/1660-4601/16/14/2612, https://doi.org/10.3390/ijerph16142612.

Mujica, Alejandro, et al. “ADDICTION by DESIGN: Some Dimensions and Challenges of Excessive Social Media Use.” *Medical Research Archives*, vol. 10, no. 2, 2022, https://doi.org/10.18103/mra.v10i2.2677.

Pascaul, Al, and Kyle Marchini. “2018 Child Identity Fraud Study.” *Javelin*, 24 Apr. 2018, javelinstrategy.com/research/2018-child-identity-fraud-study.

Paulus, Martin P., et al. “Screen Media Activity and Brain Structure in Youth: Evidence for Diverse Structural Correlation Networks from the ABCD Study.” *NeuroImage*, vol. 185, Jan. 2019, pp. 140–153, www.sciencedirect.com/science/article/abs/pii/S1053811918320123, https://doi.org/10.1016/j.neuroimage.2018.10.040.

Post, Rachael. “Friend or Foe? The Rise of Online Advertising Aimed at Kids.” *The Guardian*, The Guardian, 28 Feb. 2014, www.theguardian.com/sustainable-business/digital-online-advertising-children-privacy.

PRIVO. “History of COPPA Violations.” *Www.privo.com*, 19 Dec. 2022, www.privo.com/history-of-coppa-violations.

Rhodes, Samuel C. “Filter Bubbles, Echo Chambers, and Fake News: How Social Media Conditions Individuals to Be Less Critical of Political Misinformation.” *Political Communication*, vol. 39, no. 1, 1 May 2021, pp. 1–22, https://doi.org/10.1080/10584609.2021.1910887.

Singh, Maanvi. “Utah Bans Under-18s from Using Social Media Unless Parents Consent.” *The Guardian*, 24 Mar. 2023, www.theguardian.com/us-news/2023/mar/23/utah-social-media-access-law-minors.

Smedley, Brian D, et al. “Inequality in Teaching and Schooling: How Opportunity Is Rationed to Students of Color in America.” *Nih.gov*, National Academies Press (US), 2016, www.ncbi.nlm.nih.gov/books/NBK223640/.

"Socialmedia.utah.gov | Utah Protecting Minors Online." *Socialmedia.utah.gov*, socialmedia.utah.gov/.

Strauss, Valerie. "Perspective | Today's Kids Might Be Digital Natives — but a New Study Shows They Aren't close to Being Computer Literate." *Washington Post*, 16 Nov. 2019, www.washingtonpost.com/education/2019/11/16/todays-kids-may-be-digital-natives-new-study-shows-they-arent-close-being-computer-literate/.

"SuperAwesome Launches Kid-Safe Filter to Prevent Online Ads from Stealing Children's Personal Data." *SuperAwesome*, www.superawesome.com/superawesome-launches-kid-safe-filter-to-prevent-online-ads-from-stealing-childrens-personal-data/.

Sweney, Mark. "More than 80% of Children Lie about Their Age to Use Sites like Facebook." *The Guardian*, The Guardian, Dec. 2017, www.theguardian.com/media/2013/jul/26/children-lie-age-facebook-asa.

"Verifiable Parent Consent: The State of Play." *Https://Fpf.org/*, fpf.org/verifiable-parental-consent-the-state-of-play/.

Vogels, Emily A., et al. "Teens, Social Media and Technology 2022." *Pew Research Center: Internet, Science & Tech*, 10 Aug. 2022, www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022.

"Who Knows What about Me?" *Children's Commissioner for England*, Nov. 2018, www.childrenscommissioner.gov.uk/digital/who-knows-what-about-me/.

James, C., Weinstein, E., & Mendoza, K. (2021). Teaching digital citizensin today's world: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum. (Version 2). San Francisco, CA: Common Sense Media

Robb, M.B., & Mann, S. (2023). Teens and pornography. San Francisco, CA: Common Sense

Hern, Alex, and David Pegg. "Facebook Fined for Data Breaches in Cambridge Analytica Scandal." *The Guardian*, The Guardian, 4 Apr. 2019, www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal.

Steinberg, Laurence, et al. "Are Adolescents Less Mature than Adults?: Minors' Access to Abortion, the Juvenile Death Penalty, and the Alleged APA "Flip-Flop."" *American Psychologist*, vol. 64, no. 7, 2009, pp. 583–594, https://doi.org/10.1037/a0014763.
https://www.apa.org/pubs/journals/releases/amp-64-7-583.pdf

Age Appropriate design:

Team, Privacy Research. "An Overview of the California Age-Appropriate Design Code Act (ADCA)." *Security*, 22 Sept. 2022, securiti.ai/california-age-appropriate-design-code-act/#:~:text=The%20California%20Legislature%20enacted%20the.

Office, U. S. Government Accountability. "Federal Data Transparency | U.S. GAO." *Www.gao.gov*, www.gao.gov/federal-data-transparency#:~:text=Increasing%20the%20availability%20of%20federal.

Bob. "Cost of Cyber Security for Small to Midsized Businesses." *Imagine IT*, 26 Oct. 2022, imagineiti.com/how-much-does-cybersecurity-cost-for-small-to-mid-sized-businesses/.

Feldman, Heidi M. “How Young Children Learn Language and Speech.” *Pediatrics in Review*, vol. 40, no. 8, Aug. 2019, pp. 398–411, https://doi.org/10.1542/pir.2017-0325.

Post, Rachael. “Friend or Foe? The Rise of Online Advertising Aimed at Kids.” The Guardian, 28 Feb. 2014, www.theguardian.com/sustainable-business/digital-online-advertising-children-privacy.

-