

# xUnderstanding Children’s Privacy Implications Due to Age-Appropriate Design Codes

Authors: Cybele Greenberg , Varun Rao , Morgan Nanez

## TABLE OF CONTENTS

<b>TABLE OF CONTENTS</b>	<b>0</b>
<b>1. Introduction (Cybèle)</b>	<b>2</b>
<b>2. Policy Context (Cybèle)</b>	<b>2</b>
2.1 Policy Overview	2
2.2 Children's Online Privacy Protection Act (COPPA)	3
2.3 Children's Internet Protection Act (CIPA)	4
2.4 California Consumer Privacy Act (CCPA)	4
2.5 U.K. ‘Children’s Code’	5
2.6 California’s Age-Appropriate Design Code (AADC)	6
<b>3. Research Questions (Cybèle)</b>	<b>7</b>
<b>3. Related Research</b>	<b>7</b>
3.1 Research on COPPA (Cybèle, Varun)	7
3.2. UK Children’s Code (Morgan)	8
<b>4. Methods</b>	<b>9</b>
4.1 Methods Overview (Varun)	9
4.2 Website Data Collection and Annotation	9
4.2.1 Sampling Websites Based on Popularity (Varun)	9
4.2.2 Sampling Websites Based on Age (Morgan)	10
4.2.3 Data Annotation Process (Varun)	10
4.2.4 Threats to Validity (Varun)	11
4.3 Interviews with Industry Leaders and ICO Representatives (Cybèle)	11
4.3.1 The Princeton Internal Review Board (IRB) Process	11
4.3.2 Interviews with Industry Leaders	11
4.3.3 Limitations of Industry Interviews	13
4.3.4 Interviews with ICO Representatives	14

4.3.5 Limitations of ICO Interviews	15
4.4 Alternative Methodologies Considered (Cybèle)	15
<b>5. Results</b>	<b>16</b>
5.1 Website Data	16
5.1.1 Based on Popularity (Varun)	16
5.1.1.1 US Websites	16
5.1.1.2 UK Websites	22
5.1.2 Based on Age (Morgan)	23
5.1.2.1 US Websites	23
5.1.1.2 UK Websites	27
5.2 Interviews with Industry Leaders and ICO Representatives (Cybèle)	29
5.2.1 Industry Interviews	29
5.2.2 Industry Case Study	29
5.2.3 ICO Interviews	32
<b>6. Discussion (Entire Team)</b>	<b>34</b>
<b>7. Policy Recommendations (Entire Team)</b>	<b>37</b>
<b>8. Conclusion (Varun)</b>	<b>38</b>
<b>Appendix:</b>	<b>39</b>
A1. Copy of Interval Review Board (IRB) Application (Entire Team)	39
A2. CSV Files of Website Annotations (Morgan, Varun)	39
A3. Screenshot of Interview Contact Log (Cybèle)	39

# 1. Introduction (Cybèle)

This research project seeks to help California leaders and lawmakers to better understand the potential impact of the new California Age-Appropriate Design Code Act (AADC) on both users and businesses by analyzing some of the effects of its U.K. inspiration, the Information Commissioner's Office's Age-Appropriate Design Code (the 'Children's Code').

The project compares U.K. and U.S. user experiences across a wide sampling of websites to assess the nature and scope of new age gating measures businesses have imposed on their U.K. users to comply with the U.K.'s Children's Code. The project supplements this data with an industry case study featuring a phone interview with the chief legal representative of a major corporation to better understand how some businesses with high-traffic websites might interpret the language and applicability of the Children's Code, how they chose which age verification methodologies to use, and what plans they have, if any, to implement similar changes for their U.S. users to comply with California's AADC. Finally, the project includes insights and data from the U.K.'s Information Commissioner's Office (ICO) regarding information it has gathered thus far on the impact of the Children's Code on various online services in the U.K., and compares this information to the data collected from websites and interviews.

## 2. Policy Context (Cybèle)

### 2.1 Policy Overview

The time American children and teenagers are spending online and on social media applications is dramatically increasing. A survey published in March 2022 by the nonprofit research organization Common Sense Media and further highlighted by *The New York Times* demonstrated that in the aftermath of the COVID-19 pandemic, screen usage among teenagers had increased by 17% from 2019 to 2021.<sup>1</sup> This means it is more important than ever to protect children against a plethora of documented threats from online services, including sexual exploitation; age-inappropriate content that is violent, sexual, and/or incites self-harm; manipulative advertising methods correlated with an increase in behavioral issues such as hyperactivity and attention deficit disorders<sup>2</sup>; and the invasive and dangerous data collection, use, and sharing of children's personal information.

The following pages explain and dissect the most prominent laws within the U.S. in effect today regarding the protections of minors online. The laws that came before California's AADC – the laws that still govern the majority of data and privacy protections for children online today in the

---

<sup>1</sup> Melinda Wenner Moyer, "Kids as Young as 8 Are Using Social Media More Than Ever, Study Finds," *The New York Times*, March 24, 2022. <https://www.nytimes.com/2022/03/24/well/family/child-social-media-use.html>.

<sup>2</sup> Yair Bennett et al., "Primary Care Diagnosis and Treatment of Attention-Deficit/Hyperactivity Disorder in School-Age Children: Trends and Disparities During the COVID-19 Pandemic," *Journal of Developmental & Behavioral Pediatrics* 43, no. 7 (September 2022): 386–92, <https://doi.org/10.1097/DBP.0000000000001087>.

rest of the country – offer significantly less protections than the AADC. To best understand the intent and the innovations of the AADC, it is critical to understand some of the gaps that still persist in federal regulations on this subject.

## 2.2 Children's Online Privacy Protection Act (COPPA)

Before the California AADC was signed into law on September 15, 2022, the main U.S. law governing American children's online usage was the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6505 (“COPPA”). Broadly speaking, this law required certain websites and other online services targeted towards users under age 13 to obtain parental consent before collecting and using children's personal information.<sup>3</sup>

In 2013, the Federal Trade Commission (FTC) issued additional guidance to clarify the scope of the law and update some of its technical language to ensure the law was up-to-date with the current usages and applications of new technologies. The FTC explained that COPPA “prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.”<sup>4</sup> A “child” continued to be defined as someone under the age of 13. The “collection, use, and/or disclosure of personal information” cast a wide net, including “[requesting], prompting, or encouraging a child to submit personal information online,” “[enabling] a child to make personal information publicly available in identifiable form,” and “[passively] tracking [...] a child online.”<sup>5</sup> COPPA was meant for “operators” – defined as “any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users” – whose online services were “directed to children.”<sup>6</sup> It mandated that operators “[obtain] verifiable consent” from a child's parent or legal guardian, which meant the parent or legal guardian would “[receive] notice of the operator's personal information collection, use, and disclosure practices” and “[authorize] any collection, use, and/or disclosure of the personal information” prior to the operator's actual collection of any information on the child.<sup>7</sup>

Although COPPA was undeniably an important step in the right direction, it did leave many gaps, especially for children aged 13 and older, and for all children accessing online services that were not specifically targeted to them. This loophole has allowed businesses not specifically geared towards children to turn a blind eye to the fact that many children still use their site– a

---

<sup>3</sup> U.S. Code of Federal Regulation, “16 CFR Part 312 -- Children's Online Privacy Protection Rule,” accessed September 24, 2022, <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312>.

<sup>4</sup> Federal Trade Commission, “78 FR 3971,” accessed December 21, 2022, <https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule>.

<sup>5</sup> Federal Trade Commission, “78 FR 3971,” accessed December 21, 2022, <https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule>.

<sup>6</sup> Federal Trade Commission, “78 FR 3971,” accessed December 21, 2022, <https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule>.

<sup>7</sup> Federal Trade Commission, “78 FR 3971,” accessed December 21, 2022, <https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule>.

phenomenon that has enabled the collection and dissemination of the private information of many more children than it might seem at first glance. Although a handful of federal laws that came after COPPA continued trying to increase protections for children, COPPA has remained the main authority for most businesses operating in the U.S. offering online services – until the enactment of the California AADC.

## 2.3 Children's Internet Protection Act (CIPA)

In 2000, Congress enacted the Children's Internet Protection Act (CIPA). This law was much more narrow in scope than COPPA, but supplemented COPPA's intent to create an online environment that was safer for children. At the time, one of the greatest concerns regarding children's online activity was the threat of porn or other forms of obscene images and information. CIPA directly addressed this concern. According to the Consumer Guide published by the Federal Communications Commission (FCC), CIPA "[imposed] certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries."<sup>8</sup> These requirements included writing and adopting an "Internet safety policy" that addressed issues such as "[access] by minors to inappropriate matter on the Internet" and "[measures] restricting minors' access to materials harmful to them."<sup>9</sup> These schools and libraries also had to implement "protection measures" that would "block or filter Internet access to pictures that are [...] obscene," [...] "child pornography," or otherwise "harmful to minors."<sup>10</sup>

## 2.4 California Consumer Privacy Act (CCPA)

California has long been a leader in online consumer privacy protection. The California Privacy Protection Agency, established in 2020, is responsible for the oversight and enforcement of the California Consumer Privacy Act (CCPA) of 2018, legislation that requires businesses operating in California to make certain disclosures to their consumers in a specified manner regarding information rights and privacy protections.<sup>11</sup> The CCPA also includes specific provisions and additional protections for minors. While adult consumers retain the right to "opt-out" of the sale of their personal information by a company to third parties, minors retain the more protective right to "opt-in": "a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent

---

<sup>8</sup> "Children's Internet Protection Act (CIPA)," Federal Communications Commission, accessed December 21, 2022, <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>

<sup>9</sup> "Children's Internet Protection Act (CIPA)," Federal Communications Commission, accessed December 21, 2022, <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>

<sup>10</sup> "Children's Internet Protection Act (CIPA)," Federal Communications Commission, accessed December 21, 2022, <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>

<sup>11</sup> California Legislature, "California Consumer Privacy Act of 2018," accessed September 24, 2022, [https://leginfo.ca.gov/faces/codes\\_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5](https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5)

or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information.”<sup>12</sup>

In 2018, Governor Jerry Brown also signed the Parent's Accountability and Child Protection Act. This law requires businesses selling online products or services to consumers in California to take “reasonable steps, as specified, to ensure that the purchaser is of legal age at the time of purchase or delivery, including, but not limited to, verifying the age of the purchaser.”<sup>13</sup>

## 2.5 U.K. ‘Children’s Code’

In 2020, the U.K. adopted the Age-Appropriate Design Code, which also became known as the ‘Children's Code.’ This Code was designed to build on and enhance the U.K.’s General Data Protection Regulation (GDPR). It provides 15 standards around children’s privacy and protection online that companies operating in the U.K. and/or processing the data of U.K. children are required to follow in order to remain in compliance. These 15 standards include guidance regarding: the “Best interests of the child,” “Data protection impact assessments (DPIA),” “Age appropriate application,” “Transparency,” “Detrimental use of data,” “Policies and community standards,” “Default settings,” “Data minimisation,” “Data sharing,” “Geolocation,” “Parental controls,” “Profiling,” “Nudge techniques,” “Connected toys and devices,” and “Online tools.”<sup>14</sup>

Among other requirements, companies need to automatically turn on the highest possible privacy settings for children, attempt as best as possible to ascertain the age of a user by providing appropriate age verification mechanisms, turn off geolocation services that track someone’s whereabouts, and include nudges for children to take breaks from electronics rather than continue streaming, gaming, or using social media platforms.<sup>15</sup> One of the key aspects of this law is that it doesn’t only apply to companies offering online services that specifically target children; instead, it applies to “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services” that is “likely to be accessed by children.”<sup>16</sup>

The Code took effect in September 2021, and the ICO is currently conducting voluntary audits on several companies that offer online services in order to better understand the effects of the law so far within the U.K. The ICO is also currently investigating potential violations of the Code and considering pursuing further law enforcement action against the corporations responsible for

---

<sup>12</sup> California Legislature, “California Consumer Privacy Act of 2018,” accessed September 24, 2022, [https://leginfo.ca.gov/faces/codes\\_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5](https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5).

<sup>13</sup> California Legislature, “AB-1138 Social Media: The Parent’s Accountability and Child Protection Act,” accessed September 24, 2022, [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=20190200AB1138](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=20190200AB1138).

<sup>14</sup> Information Commissioner’s Office, “Introduction to the Age appropriate design code,” accessed December 22, 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.

<sup>15</sup> Information Commissioner’s Office, “Introduction to the Age appropriate design code,” accessed December 22, 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.

<sup>16</sup> Information Commissioner’s Office, “Introduction to the Age appropriate design code,” accessed December 22, 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.

these violations.<sup>17</sup> The results of the voluntary audits and associated studies will be released in March 2023. The interviews conducted with ICO representatives throughout this project yielded some of the preliminary data and broad trends that will be published in full then.

## 2.6 California's Age-Appropriate Design Code (AADC)

The new California legislation, modeled off the U.K.'s Children's Code of 2020, promises to provide much stricter protections for minor users than either COPPA or the CCPA. The AADC, set to go into effect on July 1, 2024, borrows exact language from the U.K.'s Children's Code and compels all businesses offering online services in California "likely to be accessed by children" (users less than 18 years of age) to fulfill a series of requirements. These requirements include estimating the age of child users "with a reasonable level of certainty," configuring all default privacy settings of child users to the highest possible level of privacy, and conducting Data Protection Impact Assessments prior to the launch of any new service or product offered online to determine and mitigate "any risk of material detriment to children."<sup>18</sup>

The AADC's relatively vague language and potential far-reaching effects have spurred significant criticism from a broad swath of stakeholders, from academic researchers to industry leaders. Most criticism is centered on the difficulty of accurately estimating the age of online users and on the high financial and operational burdens businesses may face when it comes to implementing these new age verification and compliance measures.<sup>19</sup> In an editorial published in August 2022 in *Capitol Weekly*, Eric Goldman, a law professor at Santa Clara University, takes this criticism one step further and argues the AADC will trigger an increase in invasive and prohibitive age authentication processes for all users and a dramatic shrinking of the internet for children in California, something that will eventually result in educational and professional disadvantages.<sup>20</sup>

In December 2022, the technology industry group NetChoice filed a lawsuit against the State of California in protest of the AADC, claiming that the new law violates the First Amendment by forcing private corporations to inappropriately censor speech online.<sup>21</sup> Interestingly, NetChoice includes several companies – such as Amazon, Google, Meta, and TikTok – that have already publicly made statements about recent changes to their privacy policies that enable higher levels of protection for children using online services. It seems as though many of these companies are

---

<sup>17</sup> Information Commissioner's Office, "ICO could impose multi-million pound fine on TikTok for failing to protect children's privacy," September 26, 2022, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-could-impose-multi-million-pound-fine-on-tiktok-for-failing-to-protect-children-s-privacy/>

<sup>18</sup> California Legislature, "AB-2273 The California Age-Appropriate Design Code Act," accessed September 24, 2022, [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=202120220AB2273](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273).

<sup>19</sup> Natasha Singer, "Sweeping Children's Online Safety Bill Is Passed in California," *The New York Times*, August 30, 2022, sec. Business, <https://www.nytimes.com/2022/08/30/business/california-children-online-safety.html>.

<sup>20</sup> Eric Goldman, "The Plan to Blow up the Internet, Ostensibly to Protect Kids Online," *Capitol Weekly*, August 18, 2022, <https://capitolweekly.net/the-plan-to-blow-up-the-internet-ostensibly-to-protect-kids-online/>.

<sup>21</sup> Cat Zakrzewski, "Tech industry group sues to block California children's safety law," *The Washington Post*, December 14, 2022, <https://www.washingtonpost.com/technology/2022/12/14/california-internet-lawsuit-filed/>.

claiming to be compliant with the latest applicable laws while nevertheless fighting for less regulation around this issue.

With the AADC signed into law, the primary task now facing California lawmakers is to estimate and plan for the impact of the new law on users and businesses.

### 3. Research Questions (Cybèle)

This research project seeks to help close this information gap and arm California lawmakers with a better understanding of the potential impact of the AADC on users and businesses by analyzing some of the effects of the law's U.K. inspiration, the Children's Code. The study will ask three primary research questions:

1. How do websites, applications, and other businesses offering online services in the U.K. think about whether the Children's Code applies to them?
2. If these businesses do consider themselves under the governance of the Children's Code, what changes have they made to ensure compliance with the new privacy regulations?
3. How do these changes compare to the way these same businesses currently operate in the U.S.?

The project's goal will be to empower California leaders to better predict the nature and scope of the AADC's potential effects and to alleviate some industry apprehension around these effects. Full buy-in from the technology industry is essential for the successful implementation of the AADC and the effective protection of children across the state.

### 3. Related Research

#### 3.1 Research on COPPA (Cybèle, Varun)

There has also been some limited legal academic research and policy analysis done on the effectiveness and impact of COPPA on American online businesses and their child consumers. Most research indicates that COPPA has had lukewarm results at best. This research is helpful to better understand both the shortcomings of older legislation aimed at increasing online protections for children, as well as the urgent need for more comprehensive child protection regulation. One study published in 2001 found that out of 162 websites exhibiting at least some



child content, 90% had posted privacy policy links in accordance with COPPA's guidelines.<sup>22</sup> However, the study also found that half those privacy policies were incomprehensible and failed to include several pieces of information required by COPPA, including a parent's right to review and remove their child's private information from a site.

Another study published shortly thereafter echoed these findings, highlighting discrepancies between COPPA's theoretical aspirations and its real-world implementation. A study published in 2010 found that COPPA is largely ineffective due to failed age screening mechanisms and the largest portion of teenage internet users falling outside the scope of the law.<sup>23</sup> The author called for COPPA to be revised "through the lens of social networking sites" to include "adequate notice of the uses of personal information online [...]" and a meaningful opportunity to consent to those practices."<sup>24</sup>

Other academic research concerning COPPA from the computer science community has focused on automated ways to detect COPPA violations in mobile apps<sup>25, 26</sup>, and expose privacy vulnerabilities of smart toys in violation of COPPA.<sup>27</sup>

### 3.2. UK Children's Code (Morgan)

As the U.K. Children's Code is relatively new, there is currently a dearth of information on its effects on users and businesses and very limited research into the subject. Perhaps most relevant are the ongoing audits and investigations by the U.K. Information Commissioner's Office into how various businesses are complying with the Children's Code.<sup>28</sup> It is worth noting, however, that the primary purpose of these investigations is law enforcement rather than academic, and that our project will offer a different perspective by comparing the experiences of users in the U.K with the experiences of those in the U.S across a broader swath of websites and applications.

The U.K. Children's Code and the California AADC aspire to create opportunities of notice and informed consent by requiring stricter age verification measures and privacy protections for all underage users. Although researchers and policy analysts cannot yet comprehensively assess the merit and impact of these laws, this proposed research project will attempt to start filling in some

---

<sup>22</sup> Joseph Turow, "Privacy Policies on Children's Websites: Do They Play by the Rules?," *The Annenberg Public Policy Center of the University of Pennsylvania*, Report Series, 2001, [https://repository.upenn.edu/cgi/viewcontent.cgi?article=1412&context=asc\\_papers](https://repository.upenn.edu/cgi/viewcontent.cgi?article=1412&context=asc_papers).

<sup>23</sup> Anita L. Allen, "Minor Distractions: Children, Privacy and E-Commerce," *Hous. L. Rev.* 38, no. 3 (2001), <https://houstonlawreview.org/article/4082-minor-distractions-children-privacy-and-e-commerce>.

<sup>24</sup> Lauren A. Matecki, "COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era," *Nw.J. L. & Soc. Pol'y*, 369, 5, no. 2 (2010), <http://scholarlycommons.law.northwestern.edu/njlsp/vol5/iss2/7>.

<sup>25</sup> Zimbeck, Sebastian, et al. "Automated analysis of privacy requirements for mobile apps." 2016 AAAI Fall Symposium Series. 2016.

<sup>26</sup> Reyes, Irwin, et al. "Won't somebody think of the children?" examining COPPA compliance at scale." The 18th Privacy Enhancing Technologies Symposium (PETS 2018). 2018.

<sup>27</sup> Apthorpe, Noah, Sarah Varghese, and Nick Feamster. "Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA." 28th USENIX security symposium (USENIX security 19). 2019.

<sup>28</sup> Information Commissioner's Office, "Children Are Better Protected Online in 2022 than They Were in 2021 - ICO Marks Anniversary of Children's Code" (ICO, September 7, 2022), <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/>.

of these information gaps by elucidating the nature and scope of the new age gating measures implemented in the U.K over the past year.

## 4. Methods

### 4.1 Methods Overview (Varun)

We use two complementary methods to investigate our research questions. Our primary methodology consists of analyzing the user sign-up experience and age gating measures used by websites across the US and UK, before and after the implementation of the UK Children’s Code. Our secondary methodology consists of conducting semi-structured interviews with a leading compliance representative from one of the websites identified, as well as with representatives from the U.K. ICO’s office, in order to supplement the data gathered in our primary methodology. Below, we describe each of our methods in greater detail.

### 4.2 Website Data Collection and Annotation

#### 4.2.1 Sampling Websites Based on Popularity (Varun)

We sampled a list of the 30 websites based on popularity, measured by the percentage of traffic share as reported by SimilarWeb<sup>29</sup> in September 2022 across desktop and mobile devices in the US.

We chose to use the ranking list of SimilarWeb as opposed to other data sources available for popularity/ranking and audience composition of websites for the following reasons - existence of traffic share percentage to enable our sampling strategy, accounting for both mobile and desktop traffic in the traffic share percentage, and filtering based on country.

We included 10 websites each, sampled according to their traffic share percentage, as is present in the table below:

<b>Traffic Share %</b>	<b>Websites</b>
> 0.5	google.com, youtube.com, facebook.com, amazon.com, yahoo.com, twitter.com, wikipedia.com, instagram.com, reddit.com, espn.com
0.25-0.5	linkedin.com, netflix.com, nytimes.com, cnn.com, duckduckgo.com, walmart.com, weather.com, quora.com, pinterest.com, tiktok.com
<0.25	fandom.com, indeed.com, twitch.tv, worldstar.com, t-mobile.com, hulu.com, usps.com, craigslist.org, paypal.com, imdb.com

---

<sup>29</sup> <https://www.similarweb.com/top-sites/>

--	--

#### 4.2.2 Sampling Websites Based on Age (Morgan)

In addition to sampling by popularity, we also sample a list of 30 websites distinguished by intended audience type– Adult, General Public and Child. To determine the category the website belongs to, we focused on who products/services were marketed to. For example, home depot provides hardware and home improvement goods, therefore their target audience will be adults. Pbskids, on the other hand, host a variety of educational games and resources, targeted towards children, and is therefore appropriately placed under the Child umbrella.

We included 10 websites each, sampled according to their audience type, as is present in the table below:

<b>Intended Audience</b>	<b>Websites</b>
Adult	homedepot.com, bankofamerica.com, craigslist.org, titosvodka.com, victoriasecret.com, lululemon.com, pge.com, knifeworks.com, aa.com, ncl.com
General Public	youtube.com, google.com, facebook.com, instagram.com, yahoo.com, wikipedia.com, tiktok.com, reddit.com, netflix.com, twitch.tv
Child [<18 years old]	Peeandthebigwideworld.com, pbskids.org, coolmath.com, timeforkids.com, kids.nationalgeographic.com, starfall.com, funbrain.com, disneyjunior.disney.com, nickjr.com, thekidzpage.com

#### 4.2.3 Data Annotation Process (Varun)

For each website sampled we collected the following data:

- If available, the minimum age required for sign up
- Information collected from users during sign up including username, email address, phone number, gender, date of birth, age, and security questions. We also noted whether authentication through external website accounts like google, facebook, apple, and amazon was allowed.
- Description about age in privacy policy
- Description about age in terms of use
- Disclosures about CCPA

We collected this data from the US and UK website locales in Nov - Dec 2022. Data collection for the UK locale of the websites was done through the use of a VPN. Additionally, for websites sampled based on popularity, we used the Internet Archive's Wayback Machine for collecting static content (age information contained in the privacy policy and terms of use) which was effective on or before 1 September 2021, when the UK Children's Code was fully rolled out.<sup>30</sup>

#### 4.2.4 Threats to Validity (Varun)

As is expected in any study like ours, there are limitations to our methods. We list them below.

- Website Sampling Bias: Our website sampling strategy may introduce unintended biases.
- Omitting mobile apps: The children's privacy laws are not only applicable to websites but also mobile apps. Our study focuses on websites, however, we leave mobile apps to future study.
- Unavailability of website data on internet archive: The Internet archive's wayback machine isn't able to capture dynamic content like dialog boxes used for sign ups, but works well for static content like privacy policy pages and terms of use. However, some of these static pages may not be cached for the period we are interested in.

### 4.3 Interviews with Industry Leaders and ICO Representatives (Cybèle)

#### 4.3.1 The Princeton Internal Review Board (IRB) Process

The intent of including interviews within the scope of this project is to supplement the data gathered through the primary methodology of stratified sampling with some more qualitative narrative information. Prior to being authorized to conduct interviews, the research team submitted a detailed explanation of the nature, scope, and content of the planned interviews to the Princeton Internal Review Board (IRB). A copy of the team's IRB application is included in the Appendix of this report. The research team received approval to move forward with the interviews on Friday, December 9, 2022. All interview subjects signed consent forms acknowledging the study's privacy policy prior to being interviewed.

#### 4.3.2 Interviews with Industry Leaders

We reached out to and followed up with 53 of the leading compliance, legal, and/or privacy policy experts and representatives of the companies analyzed during the stratified sampling portion of the project (see section 4.2) via either email or LinkedIn to request to conduct semi-structured interviews (see the Appendix for a full contact log detailing the outreach done on specific dates to specific industry experts). If the representative's email was readily available on

---

<sup>30</sup> "Children are better protected online in 2022 than they were in 2021" - ICO marks anniversary of Children's code (ICO, September 2, 2022)

<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/#:~:text=The%20Children's%20code%20was%20fully,protected%20within%20the%20digital%20world.>

the company website, this was our primary method of contact. If the representative's email was not readily available, we reached out to the representatives via LinkedIn Premium, as well as via the LinkedIn Sales Navigator Platform – a platform that allows up to 50 *In Mail* messages per month (the maximum possible across LinkedIn) to accounts that are not yet connected to one's own LinkedIn.

The interview questions were pre-planned. In general, they were oriented around the following themes: their familiarity with both the U.K. Children's Code as well as with the California AADC; whether and how the business came to consider itself as falling under the governance of the Children's Code and/or the AADC; their interpretation of the legal language "likely to be accessed by children" used in both laws; age verification methodology used; consideration of alternative age verification methods; challenges faced in implementing new age verification methods; plans to implement similar and/or additional age verification methods for U.S. users over the course of the next two years.

Screenshots of the pre-planned questions for the semi-structured industry interviews are included here below:

*Part 1: Role & responsibilities of interviewee at company:*

- For the purposes of better understanding your specific position at [insert company name], what is your title?
- As [insert title], what are some of your main daily responsibilities?

*Part 2: Company interpretation of Age-Appropriate Design Code regulations in US & UK:*

- Are you familiar with the UK's Age-Appropriate Design Code (the 'Children's Code')?
- What do you think of the Code?
- Do the regulations apply to your company?
- Which aspect of the regulations apply to your company?
- Which aspects of the regulations don't apply to your company?
- Are you familiar with California's new Age-Appropriate Design Code (AADC) Act?
- What do you think of the CAADCA?
- Do the new regulations apply to your company?
- Which aspect of the regulations apply to your company?
- Which aspects of the regulations don't apply to your company?
- What is the process for thinking through and implementing the regulations?

Both laws claim to cover any online service "likely to be accessed by children." How do you interpret this language?

*Part 3: Company current & projected age verification processes and procedures:*

- Does your company currently use age verification measures for your online services?
  - If no:
    - Why not?
    - What alternative processes does your company have in place to ensure it remains in compliance with the UK's Age-Appropriate Design Code (the 'Children's Code') when it comes to its UK user base?
    - Do you have plans to implement any new age verification processes prior to the CAADC's implementation deadline of July 1, 2024?
  - If yes:

- How have you implemented the U.K. Children's Code?
- How are you planning on implementing the CAADCA?
- Do you anticipate any differences in the implementation of the California and UK laws?
- What type of age verification methods does your company use?
  - Is the verification website-based or platform-based?
  - Is the verification manual or automated?
- How long have these verification measures been in place?
- Prior to the implementation of these age verification measures, did you consider any alternative age verification methodologies?
- How did you settle on this specific type of age verification?
- Will you implement any new or different age verification methods in anticipation of the AADC taking effect in 2024?
- How accurate would you consider your company's age verification methods to be, as they currently stand?
- What challenges have you faced in implementing age verification methods?
  - An example would include a reduction of user engagement
- Most age verification methodologies entail at least the temporary collection of more user information in order to predict user age. How do you think about the tradeoff between accurate age verification and privacy concerns?
- Do you expect the user experience to be more inconvenient? If so, is the inconvenience great enough to create any change in traffic or engagement.

As participation in these interviews was voluntary, we offered reasonable financial compensation for these representatives' time: \$20 for a 30-minute interview.

#### 4.3.3 Limitations of Industry Interviews

There were several anticipated limitations to this methodology. First, we expected that few compliance, legal, and/or privacy policy representatives would be willing to participate in our interviews as many of these individuals are not authorized by their companies to speak to outside parties on their companies' behalf, either formally or informally. Furthermore, privacy professionals at online services might be reluctant to discuss these topics with researchers as children's privacy is currently a widely discussed topic among lawmakers, and even acknowledging that one's company is aware of new regulations could be a liability in this context. This was one of the reasons this methodology was designated as secondary and supplemental from the start, rather than primary and central to the success of the project.

Additionally, the research team had to operate within relatively narrow time constraints for the interview portion of this project as the team was not able to start conducting interviews until they received IRB approval. Originally, the intent of the interviews was to carefully select only 10 representatives of the websites with the largest differences between the U.K. and U.S. user experiences, in order to leverage these differences during the interviews and specifically ask about the observed differences. However, as there were only two weeks between receiving IRB approval and the project's due date, the research team decided to reach out to a larger initial number of industry representatives in the hopes that at least 5-10 would reply positively.

We ended up reaching out to 53 individuals. Ideally, we would have wanted to reach out to an even greater pool of people but we ran up against LinkedIn platform constraints. On the LinkedIn

platform, even the type of LinkedIn account that enables the maximum amount of *In Mail* messages per month – LinkedIn Sales Navigator – caps the amount at 50 messages. If we had had more time, we would have planned to reach out to a greater number of people, as well as use multiple LinkedIn accounts to conduct this outreach in order to take advantage of the opportunity to send another 50 *In Mail* messages this month. Furthermore, more time would also have enabled us to spend a few days trying to track down professional emails, which would have provided us with an alternative – and probably more effective – means of outreach.

#### 4.3.4 Interviews with ICO Representatives

Our last and tertiary methodology consisted of requesting interviews with 2 current and 1 former U.K. ICO representatives in order to gather any insights and/or available data they might have on the impact of the Children’s Code on various online services operating in the U.K. The purpose of this request was to compare this information to the results of our audits and interviews from our primary and secondary methodologies and identify noteworthy patterns and divergences. The interviews were semi-structured, similar to the industry interviews. We identified appropriate points of contact through the project’s Principal Investigator (PI), Professor Jonathan Mayer, and reached out to them via email.

The interview questions were pre-planned. In general, they were oriented around the following themes: the ICO’s intent regarding certain verbiage in the Children’s Code; observed impact of the new law thus far on companies in the U.K.; major challenges companies are facing as they seek to get into compliance with the Code; anticipated published clarifications to the law.

Screenshots of the pre-planned questions for the semi-structured industry interviews are included here below:

Interview questions for representatives from the UK Information Commissioner's Office (ICO):

- The ICO has announced it is conducting audits of several companies offering online services to get a sense of how these companies are complying with the UK AADC. From the ICO's perspective, what has been the observed impact thus far of the Children's Code on various online services operating in the UK?
- On average, how much more resources have companies been spending on putting in new age verification measures since the Children's Code has taken effect?
- What changes have you been seeing within U.K. websites?
- What types of processes have businesses offering online services generally implemented to comply with the Code?
- What types of businesses have demonstrated a pattern of failing to comply with the new regulations?
- What methods have businesses used to get around the new regulations?
- How challenging is it to enforce the various provisions of the Code?
- From the ICO's perspective, what are the biggest challenges companies face when trying to come into compliance with the new regulations?
  - How stringent has the ICO been with enforcement, if a company fails to meet compliance?
- How might the new law be challenging the ICO?
- What, if anything, is the ICO doing to help companies further interpret the new regulations?
- Do you have any data available on the way various companies are implementing the new regulations that you would feel comfortable sharing with us for the purposes of our research project?

No financial compensation was offered to these government representatives due to their status as public servants.

#### 4.3.5 Limitations of ICO Interviews

As we would be asking some questions about ongoing ICO investigations and unpublished data, there was a risk the ICO representatives would either decline the interview, or be unwilling to answer several of the planned questions. For this portion of the project, we were wholly dependent upon what type of information this government entity was willing to share with us.

#### 4.4 Alternative Methodologies Considered (Cybèle)

In order to obtain the maximum amount of information on the effects of the U.K. Children's Code on companies operating online services in the U.K., we considered the possibility of filing a Freedom of Information Act (FOIA) request with the U.K. government aimed at receiving any available analysis or documents gathered by the ICO or other governmental entities through preliminary, audits, research, and/or past or ongoing law enforcement actions.

Ultimately, however, we decided against incorporating this research methodology into our project for two reasons. First, a practical consideration: there is a FOIA exemption for ongoing law enforcement actions, so the likelihood that we would be able to obtain much relevant information not yet currently available on the ICO's website is relatively low. Second, a consideration regarding our rapport with the ICO representatives: since we planned to contact



ICO representatives for interviews, doing so while also filing a FOIA request might have set a needlessly confrontational tone and negatively impacted our interactions.

Another alternative methodology we considered includes surveying child users in the U.K. to better understand the impact and efficiency of the new age gating processes of popular websites and applications. However, due to the increased complexities involved with navigating the Institutional Review Board (IRB) for child research subjects and this project's time constraints, we decided not to pursue this methodology.

## 5. Results

### 5.1 Website Data

#### 5.1.1 Based on Popularity (Varun)

In this section, we present our findings based on the data collected for websites in the US locale and then UK locales, during Nov- Dec 2022 and before September 2021.

##### 5.1.1.1 US Websites

#### **Data collection period of Nov-Dec 2022:**

##### **Minimum Age for Website Use:**

11/30 websites had no minimum age whereas other websites had varying minimum ages of 18 years (3/30), 16 years (2/30) and 13 years (14/30). It is to be noted here that websites without a specific minimum age for use, may have additional restrictions based on age but do not explicitly restrict use based on age.

13 years is likely the most popular minimum age due to the restrictions imposed on websites through COPPA which was implemented several years ago in 1998. More recently, in 2020, CCPA required opt-in consent of children under the age of 16 and the proposed CAADCA is expected to further raise the minimum age of website restrictions for children to 18. Most websites, however, have still only defined the minimum age for use of their service by children as 13, as was defined historically by COPPA.

##### **Sign Up Information:**

We observed that all websites which have a user sign up feature, allow creation of independent accounts through an email / username / phone number and password. Furthermore, many websites also allow sign-up through one or more of google, amazon, facebook, apple, twitter, and instagram accounts.

Surprisingly, only 6/30 (facebook, pinterest, fandom, worldstar, hulu, twitch) websites required date of birth or age details to sign-up for the service. And 2/30 (facebook, hulu) required users to self-identify their gender.

IMDb signup

Facebook Sign Up

CNN Sign Up

## Privacy Policy:

We find the following four kinds of descriptions concerning age and children's use of services in the privacy policies.

- 1) Detailed information about data collected about children with a separate children's privacy policy page

In this category of websites, there is detailed information about the type of data collected from children. There is also information about how the information collected varies as per specific groups of children - e.g. Google has separate , but very similar pages for age groups 6-8, 9-12, 13-17. They also have a separate Privacy Notice for Google Accounts and profiles managed with Family Link, for children under 13 (or applicable age in your country) ('Privacy Notice') (<https://families.google.com/familylink/privacy/child-policy/>).

Example Websites: Google, TikTok, Yahoo, ESPN and Hulu (Walt Disney Company)

- 2) Place the burden on the user with specific age restrictions

In this category of websites, the burden is on the user to ensure they adhere to the age based restrictions imposed by the website.

Example Websites: amazon, yahoo, netflix, nytimes, cnn, walmart, weather.com, quora, fandom

Amazon - “If you are under 18, you may use Amazon Services only with the involvement of a parent or guardian. We do not knowingly collect personal information from children under the age of 13 without the consent of the child's parent or guardian.”

Walmart - “Walmart’s general audience websites and mobile services are not directed to children under the age of 13 and do not knowingly collect personal information from children under the age of 13. For those websites and mobile services that are directed to children under the age of 13, that website or mobile service will explicitly state that it collects information from children.”

Twitch - “IF YOU ARE UNDER 13 YEARS OF AGE, THEN PLEASE DO NOT USE OR ACCESS THE TWITCH SERVICES AT ANY TIME OR IN ANY MANNER.”

### 3) Place the burden on the user based on age restriction in location of use

In this category of websites, the burden on the user is even more than the previous category, to ensure they are of legal age of consent for data processing in their country. The service does not provide guidance on the exact age.

Example Websites: twitter, reddit, pinterest

Pinterest - “Children under 13 are not allowed to use Pinterest. If you are based in the EEA you may only use Pinterest if you are over the age at which you can provide consent to data processing under the laws of your country.”

Twitter - “Our services are not directed to children, and you may not use our services if you are under the age of 13. You must also be old enough to consent to the processing of your personal data in your country (in some countries we may allow your parent or guardian to do so on your behalf).”

### 4) Vague descriptions -

Example Websites: DuckDuckGo, Indeed

Here the websites provide vague descriptions about who they believe their services are targeted to or say that there is no way for them to determine any information about the user.

Indeed - “The Sites are not directed at children and we do not use the Sites to knowingly solicit personal information from or market to children. If we learn that a child has provided personal information through one of the Sites, we will remove that information from our systems. We adopt a range of measures to try to ensure that we do not accept individuals who do not meet the minimum age and any other applicable age requirements.”

DuckDuckGo - “When you search at DuckDuckGo, we don't know who you are and there is no way to tie your searches together. [Last updated on 04/11/12]”

#### 5) No mention of age gating measures

These websites do not have any mention of age criteria or children in their privacy policy. However, this does not imply there is no guidance on children's use of the service. Such information may still be available in the terms of use (as we describe subsequently), or on a public blog post / press release.

Example Websites: Wikipedia, Instagram, Facebook, LinkedIn

### **Terms of Use:**

#### 1) Minimum age-specific guidelines of use, optionally based on location

In this category, the platforms define a minimum age of use which may be higher depending on the location of use. The minimum age of use based on location is often not stated. The burden is on the user to be of the correct age to use the service since there is no active verification. Most platforms fall into this category.

Example Websites - Netflix, Yahoo, CNN, NYTimes, Youtube, Twitter, Facebook, LinkedIn, Amazon, Reddit

Youtube - “You must be at least 13 years old to use the Service; however, children of all ages may use the Service and YouTube Kids (where available) if enabled by a parent or legal guardian. If you are under 18, you represent that you have your parent or guardian's permission to use the Service.”

Twitter - “In any case, you must be at least 13 years old, or in the case of Periscope 16 years old, to use the Services.”

Facebook - “Facebook requires everyone to be at least 13 years old before they can create an account (in some jurisdictions, this age limit may be higher). Creating an account with false info is a violation of our terms. This includes accounts registered on the behalf of someone under 13.”

LinkedIn - “The Services are not for use by anyone under the age of 16. To use the Services, you agree that: (1) you must be the "Minimum Age"(described below) or older; (2) you will only have one LinkedIn account, which must be in your real name; and (3) you are not already restricted by LinkedIn from using the Services. Creating an account with false information is a violation of our terms, including accounts registered on behalf of others or persons under the age of 16. “Minimum Age” means 16 years old. However, if law requires that you must be older in order for LinkedIn to lawfully provide the Services to you without parental consent (including using of your personal data) then the Minimum Age is such older age.”

Amazon - “If you are under 18, you may use the Amazon Services only with involvement of a parent or guardian. Parents and guardians may create profiles for teenagers in their Amazon Household. You must be at least 21 years of age to purchase alcohol, or use any site functionality related to alcohol.”

Reddit - “You are at least 13 years old and over the minimum age required by the laws of your country of residence to access and use the Services; You can form a binding contract with Reddit, or, if you are over 13 but under the age of majority in your jurisdiction, that your legal guardian has reviewed and agrees to these Terms;”

## 2) General restrictions based on age, without age-specific guidelines

In this category, the platforms do not specify any age-specific guidelines but provide general guidance of use putting the burden on the user to be of legal age.

Example Websites - Google, T-Mobile, Craigslist

Google - “If you’re under the age required to manage your own Google Account, you must have your parent or legal guardian’s permission to use a Google Account. Please have your parent or legal guardian read these terms with you. If you’re a parent or legal guardian, and you allow your child to use the services, then these terms apply to you and you’re responsible for your child’s activity on the services.”

T-Mobile - “When you accept, you're telling us that you are of legal age (which means you are either legally emancipated, or have reached the age of majority as defined in your jurisdiction) and that you are able to enter into a contract.”

Craigslist - “If you agree to the TOU and (1) are of sufficient age and capacity to use CL and be bound by the TOU”

### 3) No restrictions on use based on age

In this category, there are no age-specific guidelines present in the terms of use. However, such guidance may exist in the privacy policy or elsewhere on a public blog post / press release.

Example Websites - Wikipedia, Instagram, ESPN, USPS, IMDb, PayPal

### **CCPA Disclosures:**

We found that almost all the websites had disclosures about adhering to CCPA. Interestingly, Twitter did not have a CCPA disclosure.

### **Data Collection Period before Sept 2021:**

The UK Children’s Code was fully enforced in Sept 2021. To understand whether websites have made any changes to their privacy policy and terms of use pages we used the WayBack Machine and compared our findings with that observed in Nov-Dec 2022.

We observed no changes (or very minor sentence tweaks) in almost all of the websites. We note the very few exceptions below:

### **Privacy Policy:**

Google - Family Link Page did not exist

Indeed - They had specific guidance based on age and location of use in Aug 2021 (category 2,3), but had only a vague description in Nov-Dec 2022 (category 4).

“The Sites are not for use by anyone under the age of 16. However if local laws provide for an alternative minimum age for the provision of the Sites’ services to you, then that shall apply as the applicable minimum age. In all jurisdictions outside the European Union, if you are under the age of 18 or the age of majority in your jurisdiction, you must use the Sites under the supervision of your parent, legal guardian or responsible adult.”

## **Terms of Use:**

Reddit - had additional guidance for people under 18 years of age.

“In addition, certain of our Services or portions of our Services require you to be 18 years of age or older, so please read all notices and any Additional Terms carefully when you access the Services.”

### 5.1.1.2 UK Websites

## **Changes from US Locale during Nov - Dec 2022:**

In this section we report any changes observed in the UK locale in comparison to US locale during Nov - Dec 2022.

**Minimum Age for Website Use:** No change

**Sign Up Information:** Mostly no changes were observed. In the case of weather.com, while the service allowed account creation in the US locale, there was no such provision in the UK locale.

## **Privacy Policy:**

We list and discuss the websites which had changes below.

Yahoo - had detailed information about data collected about children with a separate children's privacy policy page in the US locale, but there was no mention of children in the UK locale.

Instagram - no mention of age / children in the US locale, but had a very detailed description of age based restrictions and type of data collected in the UK locale privacy policy. Here's a short excerpt:

“For people under the age of majority (under 18, in most applicable countries) who have a limited ability to enter into an enforceable contract only, where we may be unable to process your information on the grounds of contractual necessity. If you are under the age of majority in your country and there is no enforceable contract in place, we will take particular account of the fact that you are below the age of majority when conducting our assessment of our legitimate interests and the balancing of your interests and rights. We provide specific protections for people below the age of majority to ensure that they are aware of the risks, consequences, safeguards and rights associated with the processing of their information.”

TikTok - additional guidance for users under 18 years of age

“To provide users younger than 18 with an age-appropriate experience, certain features are not available. Further details are available in our Help Centre.”

Other websites that had minor word changes included CNN and Indeed.

### **Terms of Use:**

We list the websites which had differences in their terms of use below.

CNN - had separate mention of Subscription services and CNN Live

“(A) for CNN Live, you must reside within the United Kingdom, (“UK”); and  
(B) for all Subscription Services, you must be at least 18 years old, or older if the legal age of majority in your state or territory is older than 18. Individuals under the age of 18, or the applicable age of majority, may access or use the Subscription Services only under the supervision of a parent or legal guardian with a Subscription for the relevant service (each authorized individual shall be referred to in these Terms as an “Authorized User”).

TikTok - had details about specific features based on age.

“Access to certain features of the Platform depends on your age. For example:  
Direct Messaging: You must be aged 16 or older to use the direct messaging functionality.  
TikTok LIVE: You must be aged 18 or older to live stream and use live streaming features.  
Virtual Items: You must be aged 18 or older to interact with virtual items.”

### **CCPA Disclosures:**

Most websites, even if having very similar privacy policy pages compared to the US locale, the section on CCPA had been removed.

### **Comparison with UK Locale before Sept 2021:**

For those websites which had no changes in the UK locale compared to the US locale, we did not find any difference in the privacy policy and terms of use before and after implementation of the UK Children’s code. For most of the remaining websites, the privacy policy pages and terms of use were not archived.

#### **5.1.2 Based on Age (Morgan)**

In this section, we present our findings based on the data collected for websites in the US locale and then UK locales, during Nov- Dec 2022..

##### **5.1.2.1 US Websites**

### **Minimum Age for Website Use: 13**



14/30 sites had no minimum access or sign-up age. Of these 14, 7 were for sites intended for child audiences. While these 7 sites, such as kids.nationalgeographic.com, had no outright access restriction, they did implement various content related age-gating within the site itself. Of the other 17 sites– 1 restricted access to > 5 years old, 7 restricted access to > 13 years old, 2 restricted sign up or access to > 16 years, 6 restricted access or sign up to > 18 years old, and 1 restricted access to > 21 years old

Similar to the previous survey above, 13 years is likely the most popular minimum age due to the restrictions imposed on websites through COPPA which was implemented several years ago in 1998. Nearly every site also complied with CCPA. We found that most sites that offered products, such as lululemon.com, as opposed to a service, such as google.com or instagram.com, had a larger variance of age restrictions, ranging from 13-21. We believe this could be due to using SSN and credit cards on the site. Most websites, however, have still only defined the minimum age for use of their service by children as 13, as was defined in COPPA.

### **Sign Up Information:**

We observed that 25/30 sites offered account creation. These sites did not require you to have an account in order to view the site contents. Of these 25 sites, only 5 required date of birth as an input and form of manual age verification. Of these 5, only 1 was a site intended for children. However, the sites intended for children almost always prescribed the guardian or teacher to create the account for the child.

We also observed that in addition to independent sign up pages, 4 sites allowed you to create accounts via third parties, such as your apple account or google account. All of the sites that allowed third party sign-in were social media companies.

### **Privacy Policy:**

We find the following kinds of descriptions concerning age and children's use of services in the privacy policies.

- 1) Site is stated as "Not Intended" for children or minors under a specific age.

In this category, the site, regardless of sign-up mechanism or age verification methods, directly states that the contents or use of the page is not intended for children. These sites place the burden on the individual to adhere to their age restrictions. These types of sites span all 3 of our survey categories.

Example: homedepot, tiktok

2) Any age access, but age-gated content or additional restrictions

In this category of websites, anyone can access the site, but once on the site there are additional restrictions based on age. These sites are usually intended for children.

Example Websites: reddit, disneyjunior

Disneyjunior.com: Some of the features on our sites and applications are age-gated so that they are not available for use by children, and we do not knowingly collect personal information from children in connection with those features.

3) Place the burden on the user based on age restriction in location of use

In this category of websites, the burden on the user is even more than the previous category, to ensure they are of legal age of consent for data processing in their country.

Example: yahoo, american

Yahoo.com: “We do not knowingly collect, use, or share information that could reasonably be used to identify children under age 13 without prior parental consent or consistent with applicable law”

Aa.com: American does not knowingly collect personal information directly from children – persons under the age of 13, or another age if required by applicable law.

Victoriasecret.com: We do not knowingly collect or solicit personal information from children under the age of thirteen (13) (or other relevant ages, which may apply by virtue of applicable law) through our Services.

4) No mention of age gating measures

These websites do not have any mention of age criteria or children in their privacy policy. However, this does not imply there is no guidance on children’s use of the service. Such information may still be available in the terms of use (as we describe subsequently), or on a public blog post / press release.

Example Websites: knifeworks, lululemon

We also found that many of the sites geared towards children had a separate page for children's privacy policies. These pages went into further detail about how data is collected and used for children on the site. The language of the sites was intended for adults.

We also found that most of the sites had a disclosure about sharing data with third party vendors.

### **Terms of Use:**

Aside from mentioning or complying with CCPA, 17/30 sites explicitly stated that they do not knowingly or intentionally keep, collect, or share personal information from users under varying ages, typically less than 13-18. These sites state that they will delete the user data if they are found to be below the designated age. In addition to this, we found the following types of terms of services related to age.

#### 1) Minimum age-specific guidelines of use, optionally based on location

In this category, the platforms define a minimum age of use which may be higher depending on the location of use. The minimum age of use based on location is often not stated. The burden is on the user to be of the correct age to use the service since there is no active verification. Most platforms fall into this category. These sites were present in all 3 survey categories.

Example Websites - victoriasecret, lululemon, netflix

victoriasecret.com - "You agree that you will not: (i) use the Service or any services we offer ourselves or through a third party if you are **under the age of majority** in your state of residence (a minor) unless your parent or legal guardian has agreed to these Terms on your behalf and granted you permission to use the Service or any services we offer"

lululemon.com - "The Sites and Apps may be accessed and used only by individuals who can form legally binding contracts under applicable laws, who are 18 years of age or older, and who are not barred from using the Sites and Apps under applicable laws"

netfliix.com - "You must be at least 18 years of age to become a member of the Netflix service. Individuals under the age of 18 may only utilize the service with the involvement of a parent or legal guardian, under such person's account and otherwise subject to these Terms of Use."

#### 2) General restrictions based on age, without age-specific guidelines

In this category, the platforms do not specify any age-specific guidelines but provide general guidance of use putting the burden on the user to be of legal age.

Example Websites - Google, Craigslist

Craigslist - “If you agree to the TOU and (1) are of sufficient age and capacity to use CL and be bound by the TOU”

### 3) No restrictions on use based on age

In this category, there are no age-specific guidelines present in the terms of use. However, such guidance may exist in the privacy policy or elsewhere on a public blog post / press release.

Example Websites - titosvodka, pbskids

It is also worth noting that all of these sites but 1 used language not suitable or understandable for children. No other site, in any of the survey categories, was directly geared towards children.

Nickjr.com privacy policy: “You should always check with your parents or guardians before giving out any information about you, especially before entering information on any website mobile application, or online service. We consider you to be a child if you are **not of legal age to consent** to the collection and processing of your Personal Information under applicable laws where you live.”

### **CCPA Disclosures:**

We found that almost all the websites had disclosures about adhering to CCPA. 1 site intended for children and 2 sites intended for adults did not explicitly have CCPA disclosure.

#### 5.1.1.2 UK Websites

We noted that nearly every website was only hosted on U.S. sites. We observed no changes (or very minor sentence tweaks) in almost all of the websites. We note the very few exceptions below:

Google - Family Link Page did not exist

Disney Junior, Nick Jr., and American Airlines had separate UK entities, however they both still did directly specify age requirements for minors.

Lululemon and Victoria Secret have separate U.K Entities, and were the only sites newly restricting access to >18 years old, and directly stating that U.K. residents must adhere to the restriction.

### **Changes from US Locale during Nov - Dec 2022:**

**Minimum Age for Website Use:** No change

**Sign Up Information:** No change

### **Privacy Policy:**

5/30 sites had separate sections or pages for U.K laws. While no site explicitly stated the new U.K Law, lululemon reiterated that users must be > 18.

We found that many sites used vague verbiage to perhaps comply with the new law. They use blanket statements to cover all their bases.

Example:

American Airlines.” American does not knowingly collect personal information directly from children – persons under the age of 13. To the extent that American Airlines, Inc. is subject to the laws of the European Union, the United Kingdom, Switzerland, or Uruguay when processing personal data (“Personal Data”), it shall be the “data controller” under such laws.”

### **Terms of Use:**

We noted minimal differences between U.K sites and US sites.

Victoria secret was the only site to explicitly reference U.K residents in its Terms of Services.

Example:

Victoria Secret: To register on the site and to place orders with us you must be aged 18 or over and a UK resident

### **CCPA Disclosures:**

Most websites, even if having very similar privacy policy pages compared to the US locale, the section on CCPA had been removed.

## 5.2 Interviews with Industry Leaders and ICO Representatives (Cybèle)

### 5.2.1 Industry Interviews

Of the 53 industry personnel contacted, within the span of two weeks, only 5 responded with 4 declining and 1 accepting an interview. Because of this low response rate and the aforementioned time constraints for the project, we decided to shift the focus and analysis of this section of the report. Rather than conducting an analysis of the broader trends within the data we hoped to collect from at least 5-10 industry interviews (a type of analysis that doesn't really make sense anymore in this context), we decided to report the information gathered in this section as a case study centered on the one company that responded. In section 5.2.4, we compare their answers with information received from the ICO to show some examples of the challenges and disconnects between law-makers and industry.

### 5.2.2 Industry Case Study

#### *Role at the Company*

The industry expert we interviewed is the lead in-house counsel for the company's healthcare data and technology branch. In the past, he also headed the company's compliance efforts with COPPA and has remained involved with implementing new processes and review systems that ensure the company is staying compliant with any new child privacy regulations. He has advised on code writing for new products, user interface, and downstream data processing. He is a member of the company's Digital Citizenship Group, a group of specialized employees focused on enhancing the company's global governance when it comes to the data storage and collection practices of its various digital assets.

#### *Overall Company Policy Regarding Children*

He explained that overall, his company does not target children. Rather, the large majority of its marketing and advertising is geared towards the breadwinners of the family. That being said, the company has had and does still currently have some special online programming for children, and family and family values lie at the core of the business. In the past, the company launched a child-centered marketing campaign focused on toys and the upcoming Christmas holiday. Through a firewall that protected children from having their personal information tracked and saved, children could browse a list of toys online and create a wish list of the ones they liked. They could then send the wish list to an adult, and this adult could login into their online portal, enter their credit card information and check out with the toys. Although this particular program no longer exists, the company is currently pursuing a partnership with an online gaming platform to create a virtual reality program in which children can interact online with talking toys made by the company. This program is also being implemented behind a firewall to protect children's privacy and prevent the company as well as other third parties from inadvertently illegally collecting children's data. The company is getting certified by a third party to ensure it is in

compliance with COPPA— which the company still currently regards as the first and foremost online child privacy U.S. authority.

#### *Anticipated Problems with the AADC*

When asked about the U.K. Children’s Code, this attorney explained he was familiar with the law from an academic perspective, but not any more than that. The company had divested from its U.K. subsidiary a few years ago, and so he admitted they had not spent many resources on reading new U.K. policy.

The attorney was familiar with the California AADC, and had mixed opinions about it. He believed that defining “children” as anyone under 18 years old – and thus raising the age from the way COPPA currently defines it as under 13 – made sense from a legal and theoretical perspective, but not from a business or practical perspective. From a legal perspective, he claimed this was not unreasonable, as 18 is a defining status in terms of rights regarding healthcare decisions, emancipation, etc... From a business perspective, however, this age cutoff is more difficult to justify. On average by the time a minor reaches the age of 15 or 16, he or she is often already engaged in various adult-like transactions, such working a job, earning money, and owning a credit or debit card. Although the company’s privacy policy states it expects users to be above the age of 17 to complete any purchases, he admitted the company had no real way of verifying the age of a user beyond this self-certification. In light of minors being involved in various adult financial transactions online and the absence of more developed age verification measures, he believed that raising the age of a “child” online to 18 is not going to be easily enforceable for either companies or regulators.

The attorney also mentioned that one of the main ongoing issues with COPPA would also copy over into the AADC: the inability of websites to secure meaningful parental consent for the children’s online activities. He said that the AADC included language prohibiting companies from giving children access to images or other information that would be “materially detrimental to the health of the child.” But this language is very subjective, and different parents could have different definitions or standards for what should be considered detrimental to a child’s physical and mental health. According to the attorney, this problem is exacerbated by the fact that no current parental consent technology exists that can be viable at scale.

The attorney brought up one last main issue with the implementation of the AADC: the vagueness of the wording “likely to be accessed by children.” With COPPA, the intent of the company was the most important— companies could not specifically target children and collect their private information. With the AADC, however, the intent of companies is no longer what matters. Instead, what matters is whether children have the *ability* to access a given website; it’s a question of generalized opportunity and motivation. With the proliferation of smartphones and laptop computers, the language of the law makes it seem as though the presumption of almost all

websites should be that they are being accessed by children, and therefore need to ensure they are compliant with the AADC. This puts a much larger burden on companies.

### *Age Verification Methods*

Currently, the company only uses age verification measures as part of its identity verification measures for its healthcare and banking branches. The company almost exclusively employs third party entities to implement these manual identity and age verification measures. If the company had to begin actively pushing every user through age verification processes in order to comply with the AADC, it would most likely do so through a third party. The difficulty is that most third party identity verification vendors do not have verification data for users under 18 as they rely on financial information such as credit scores to successfully complete this identity verification— information that minors would not have.

One possibility that the company is exploring is a mandatory identity and age verification process for all users who sign up for an online account with the company. If this age verification was a standard part of the onboarding process, it might not seem as burdensome to users. But, requiring this amount of personal information in order to be allowed to purchase paper towels, for instance, could also seem excessive and onerous to many customers. These age gates could be disruptive to customer engagement and experience.

Another downside to age verification methodologies is that they usually require the use of a third party. Every time a third party is involved, it is impossible not to provide any data back. So, implementing more age verification processes could simply result in third party vendors and analytics firms getting access to a whole trove of invasive new data.

### *Alternatives to Age Verification*

Instead of hiring a third party vendor to create and implement a whole new age verification platform that would likely not be immediately effective, the company is considering several less burdensome alternatives that would still ensure the company is complying with the AADC as best it can. Some of these alternatives include turning off geolocation tracking for all users unless they opt to turn *on* this tracking (such as for order deliveries); clearly and actively encouraging users under the age of 18 to not provide any personal information online to the website; continue to separate out experiences targeted towards children and ensure these experiences are operating from behind a firewall.

### *Anticipated Changes Due to the AADC*

According to the attorney, the most immediate impact of the AADC on the company's website will include carefully rethinking the language and marketing materials that are publicly available on the website to any user without an account. Currently, the company thinks of itself as very family-friendly, and so there are a lot of bright colors and illustrations used. This will need to



change, as it could be interpreted to be marketed specifically towards children. The messaging around toys and electronics will need to become more clearly geared towards parents rather than children.

Another impact will be greater governance regarding the way code is developed and maintained. The company's Digital Citizenship Group will lead code reviews of new digital assets to ensure the codes avoid misleading data transfers and/or violations of privacy policies, especially with regards to children.

Lastly, the company plans to revise its privacy policy to make it very clear that the company does not target children, and that it expects users on its site to be adults.

### 5.2.3 ICO Interviews

We were able to conduct two interviews with three current and former ICO employees (one interview included two people). The following reported information is a summary of the main data points and trends that were discussed during the interviews.

#### *"A Proportionate Approach"*

One of the major themes that emerged from these interviews with ICO representatives was the ICO's intent to apply the Code *proportionally* rather than indiscriminately. Applying the Code proportionally means that websites that include heavy traffic and/or are specifically geared towards children will be expected to invest more resources into processes such as age verification, while websites with lighter traffic will only require minor adjustments to comply with the Code. Some of these minor adjustments could include a landing page that prevents accidental traffic from seeing inappropriate material, or some form of self-certification. This ICO's commitment to a proportionate approach helps clarify the language of the Code that claims to apply to all online services "likely to be accessed" by children. Low risk sites don't need a ton of age assurance. As the risk starts to go up, the ICO expects to see more efforts. A detailed DPIA is the primary document the ICO will rely upon in considering whether a company has gone to the appropriate lengths to ensure it is in compliance with the law. The ICO acknowledges that complete age assurance is currently limited by available technology. But the Code is specifically written in a way that is technologically neutral, so that as technology becomes better at identifying user age, expectations for the protection of children's data, privacy, and online activities will also increase.

#### *Balancing Age Verification with Increased Data Collection*

One of the major problems with age gating brought up by the industry representative we interviewed was that implementing age verification processes often means inevitably collecting more private information on a user – at least temporarily – either directly or through a third party. The ICO, however, believes this is a cop-out excuse by industry representatives who do not want

to put in the necessary resources to invest in child safety and privacy online. In early 2023, the ICO expects to release further guidance for companies on how to assess whether children are accessing a website with techniques that do not include formal age verification processes.

Alternative methods of making a reasonable assessment regarding the age of users could involve assessing what sorts of advertisements are on the site; checking to see whether toys or electronics used by children are linked to the site; leveraging information already incidentally collected through other means such as market research by third parties regarding the average ages of a website's users, or information gleaned from complaint channels, or even standard registration information. While there is a tension between data collection minimization and effective age verification, some high-risk sites such as pornography make implementing intrusive age gates worth it. In other words, the safety of the child might trump complete privacy and anonymity in some specific cases. This goes back to the idea of a proportionate approach to age assessment online.

#### *Results from Preliminary Audits & Analysis*

Over the course of the past year, the ICO has conducted research on the ways companies in three major sectors – social media, streaming, and gaming companies – have implemented some of the Code's new requirements. Overall, the ICO reports relatively positive results. Out of the companies contacted by the ICO, 40% were identified as low-risk for potential harm to children, and no further investigative action by the ICO was recommended. Another 40% were assessed to not quite yet be in compliance with the Code, although some efforts had been made to improve these companies' performances in this area and they were deemed overall to be on the right path. Only 20% were assessed to be in non-compliance and to require further investigations.

For each of the three major sectors, the ICO identified specific areas of improvement, as well as specific problem areas requiring more work. Social media companies have improved "suitability to children's reading age"; the "effectiveness of reporting tools"; and "measures taken to ensure third party sharing is in conformance with the code."<sup>31</sup> However, they still need more work when it comes to "profiling"; "age assurance measures"; and "transparency of privacy information." Gaming companies have improved "geolocation being off by default"; "conformance re profiling"; and "effectiveness of reporting tools." However, they still need more work on "nudge techniques"; "parental controls"; and "building in the best interest of the child into the design and development." Lastly, streaming companies have improved "geolocation being off by default"; "measures re 3rd party sharing"; and "transparency of privacy information." They still need to improve "compliance with external standards (excluding code)"; "the automatic setting of children's profiles"; and "parental controls."

---

<sup>31</sup> Exact language used by ICO representative in a follow-up email dated December 21, 2022. This reference applies to all quoted language in this paragraph.

### *Observed Changes Within U.K. Websites*

The ICO representatives noted several broad trends they had observed since the implementation of the Children's Code in September 2021. Most of the increased compliance with the Code so far has revolved around greater transparency measures, such as better privacy notices, better parental controls, changing privacy defaults to high. Such changes are easier to make than, for example, implementing full age verification processes, because they do not impact or change the core of the business, and the core of a user's experience with the website.

Lastly, companies are continuing to work on exploring more effective age assurance processes. Some are working with AI companies that can make a relatively accurate assessment of a child's age based on facial structure and shape. Others are interested in more 'neutral' age verification processes, such as pop-ups that require entering in a birthday over multiple different visits to the site to ensure a user is being truthful about their age.

## 6. Discussion (Entire Team)

### ***No Mention of Children's Code or CAADCA, unlike CCPA***

Across both surveys of websites (popularity and intended audience), we noticed minimal to zero mentions of Children's Code or CAADCA. In the U.S sites, nearly every website mentioned CCPA. Because of this, we imply that it will be feasible to also directly acknowledge California's new law on the websites.

Similarly, in the UK, we found that nearly all websites that acknowledge the U.K. law in general, had sections pertaining to Personal Data Rights, as a result of the 2018 U.K GDPR. This was interesting, as sites were able to implement this law, but lacked implementing the more recent Children's Code. Among all websites, whether geared towards children or adults, or popular or not, nearly no site indicates U.K. residents are protected under U.K Children's Law. It was surprising to find that even large companies, with exhaustive man-power, such as Facebook or Google, still do not explicitly indicate new age minimums. This gives us insights on how we should better implement and enforce the California Children's Code possibly along the lines of the GDPR.

### ***No Explicit Enforcement / Verification of User Age, With the Burden (Mostly) on Users***

We noticed that most websites place the burden of age verification on the users. For example, how Twitch's privacy policy states "IF YOU ARE UNDER 13 YEARS OF AGE, THEN PLEASE DO NOT USE OR ACCESS THE TWITCH SERVICES AT ANY TIME OR IN ANY MANNER.". These sites typically have weak age verification and do not even ask for the users date of birth when creating an account. This lack of enforcement on the website's end does not directly protect against children.

We also notice that while many sites claim users have to be a certain age to use the site, they still expect users to be dishonest by also placing statements that they will “either delete the information or immediately seek the parent’s consent.” as per Disney Junior’s Terms of Use, for example.

### ***Irregularities in Compliance***

We found it interesting how nearly all US based websites were able to have CCPA disclosure, but continue to intercept the minimum age of access to be 13, which if needed to be in compliance with CCPA would have to ideally be raised to 16.

### ***Vagueness in Descriptions and Age Estimation***

We noted that many sites used vague language when addressing age restrictions. Phrases such as “sufficient age” and “age of majority” and “under the applicable law” were used as all encompassing statements to suffice any law or age restriction.

Although several websites said they would take action if they detect underage behavior from an account, there is very little literature about how age estimation is actually done other than if it is reported by other users. Many websites claim to use third-party verification systems, while others, like Facebook, mention very vague and unclear uses of “AI”. The use of AI in age verification must be done very carefully. In order to train a model, children’s data is needed. However, sites are prohibited from collecting, and state that they do not collect data of minors or persons below a certain age. This results in a conflict where one cannot collect children’s data and therefore cannot train a model but still need to estimate children’s use of the website.

Here’s an example statement from Google:

Across Google services, if we learn that you may not be old enough to have a Google Account, you’ll have 14 days to update your account to meet age requirements or your account will be disabled.

### ***Changes Between US - UK***

Surprisingly, there were very few changes in the UK and US locale versions of the website sign-up processes, privacy policies, terms of use and general user experience (e.g. only Instagram, TikTok, Lululemon and Victoria’s Secret had noticeable changes in their privacy policies/terms of use), even though the UK Children’s Code was fully enforced for over a year. In those services where there were changes observed, we found the minimum age of use increase to 18 years of age, and more detailed information about how children’s data may be processed.

Since CAADCA has heavily borrowed language and enforcement mechanisms from the UK Children’s Code, it is reasonably likely that the enforcement of CAADCA may be similarly weak and its applicability limited as is also confirmed by the interviews with the ICO..

### ***Changes Before and After Enforcement of the Children’s Code***

Surprisingly, we did not notice many changes in either UK or US locale’s of the websites in their privacy policies before Sept 1, 2021 when the UK Children’s Code was enforced. At least for the UK locale, it appears that websites think of themselves as already compliant with the UK Children’s Code since they had made the required changes under the older GDPR in 2018.

### ***Low Response Rates for Interview Requests by Private Companies***

One notable methodological result was the overall lack of industry responses to interview requests. From this data, we can reasonably infer that privacy professionals at online services might be reluctant to discuss these topics with researchers due to the potential liability associated with even acknowledging the need to implement greater child privacy protections online. One possible policy response by government entities could be to actively encourage these companies to speak to and work with academic and government researchers to help these researchers better understand what the remaining gaps are between law-makers and industry. This encouragement could include liability protection for a certain amount of time (i.e. from now through the first year of the AADC’s implementation) to reassure companies that participating in such research will not result in bad press and/or prosecution for apparent violations. Or, encouragement could also take the form of financial incentives such as reasonable tax breaks for participating in much-needed research on this subject.

### ***Challenges and Disconnects Between Law-Makers and Industry***

Comparing the industry and ICO interviews suggests there are still many discrepancies between the intent of law-makers and the interpretation of the laws by industry professionals. The common theme within these discrepancies is a tendency by industry to dramatize and overestimate the reach and intent of the law.

The best example of this is in the interpretation of the part of the Code that explains it applies to all websites “likely to be accessed” by children. While at first glance this might seem to include most websites – especially considering the proliferation of smartphones, tablets, and other hand-held electronics among minor users – the ICO representatives revealed that they were actually taking a proportionate approach to determine what types of websites need what types of additional child protections.

Another example is the central industry concern that age verification processes are currently neither accurate nor scalable. However, the ICO interviews made it very clear that law-makers understand this and do not expect all businesses to invest large amounts of resources into cutting-edge age assurance measures. Instead, there are many alternative, less technologically advanced methods that can be used to identify whether children are using a website. These methods are expected to evolve alongside technological advances. As the AADC employs language that is almost identical to the U.K. Childrens Code, California legislators should adopt

and clarify a similar proportional approach to the expectations and to the enforcement of the AADC.

## 7. Policy Recommendations (Entire Team)

### ***Investing in Creating Better Age Verification Measures, and Balancing Data Minimization with Effectiveness***

One of the major friction points between law-makers and industry is a disconnect regarding the expectation of effective age assurance processes. Industry representatives feel anxious about the way new laws seem to imply complete age verification for all customers is required; meanwhile, law-makers claim the law is much more flexible and intended to be applied in a way that is individually tailored to each specific company. The ICO specifically claims that the Code is meant to evolve with new age verification technology as it becomes available. We recommend that companies with a large online presence continue investing in the technological development of effective age verification measures so that this challenge can eventually be overcome. Some have declared plans to incorporate AI to make age verification more effective. We recommend doing so with caution, as AI could also mean more information on children is collected and potentially stored, such as the shape of individual children's faces and other personally identifiable physical features that would enable AI to predict a child's age. In the meantime, companies should continue to employ other, less complex ways of preliminarily assessing age to protect children as best they can while technology catches up to societal expectations.

### ***More Sincere Efforts by Industry, and Clearer Implementation Guidelines and Enforcement Mechanisms from Regulators***

Given the evidence presented through websites and interviews with representatives in industry and government, in order to ensure compliance with the proposed AADC, services may opt to make some superficial changes that 'check the box' but do not actually materially improve the safety of children online. Some examples of these largely ineffective changes include:

1. Updating privacy policies and terms of use to have the minimum age of access / sign-up be 18 years of age instead of the existing 13 years, while still placing the majority of the burden on users via self-certification mechanisms. This forces users into theoretically binding privacy policies that most users do not actually read through and/or understand.
2. Editing current policy by retaining the minimum age of access, but adding in separate guidelines for users under 18. This is also mostly a 'cop-out' solution as this will not prevent children from accessing age-inappropriate content online.

While these changes are a necessary part of the solution, they are not sufficient. Companies must put more effort into changing the way users interact with websites beyond tinkering with words within dense privacy policies. On the flip side, regulators should also be conscious of the vagueness in many parts of the new laws and continuously publish more examples, checklists, and other helpful materials to help guide companies towards what right looks like.

### ***More Transparency Regarding Data Collection Practices***

We recommend regulators require greater transparency from all websites regarding their data collection practices for minor users. For example, details about what data is collected on children of various age ranges, how long this data will be retained, and what is the basis for processing it, must be made publicly available and easily accessible. When dealing with sites that are intended for only users less than 18 years of age, we suggest regulators enforce a zero data collection standard when it comes to minor users.

### ***Early Data from U.K. Should Help Alleviate Industry Fears Around the Effects of the AADC***

The interviews with ICO representatives made it clear that the expectations of regulators are much more measured and reasonable than a strict reading of some of the language within the Code might imply at first glance. California law-makers should take this into account when responding to industry push-back on the AADC and explain through clear messaging to industry that the expectations of the new regulations are individually tailored to each company based on a variety of factors such as size, user age base, amount of available resources, etc... In this same vein, California regulators should issue additional guidance as soon as possible regarding how various types of companies should interpret legal language such as “likely to be accessed by children.” Publishing more specific examples of how this language can be understood in the context of different types of companies could be a game-changer for industry acceptance of these new regulations in the U.S.

### ***Other States Should Adopt Similar Child Protection Measures***

As California law-makers work through the early challenges of implementing the AADC, they should also encourage other states to adopt similar policies. One of the challenges U.S. companies currently face is the fact that adhering to these new regulations will require a significant resource investment, and this investment becomes exponentially more worth it if more states start to get on the same page when it comes to the protection of children online. A show of solidarity by state regulators across the U.S. could significantly help increase industry motivation to put more effort into ensuring compliance with these new laws.

## **8. Conclusion (Varun)**

Our work sought to understand the potential impact of the proposed AADC on American websites and provide a body of complementary evidence that could be valuable in informing policy regarding protecting children online in America.

For over 50 websites sampled according to their popularity and intended audience, we analyzed sign-up behavior, privacy policies and terms of use of websites. To supplement this evidence, we presented a case study based on a semi-structured interview with one of the largest retailers in America and compared their responses with information received from the UK’s ICO to provide examples of the challenges and disconnects between law-makers and industry.

Our findings indicate that there was generally no mention of AADC or of the UK Children’s Code in any publicly available information provided by these services and that the burden is almost completely on the user to self-certify their age or to ensure that they are in compliance with local laws. These observations were confirmed and reinforced through interviews with industry and government regulators. Furthermore, the interviews also highlighted discrepancies between the intent of law-makers and the interpretation of the laws in industry underscoring industry’s tendency to dramatize and overestimate the scope, intent, and effects of the law.

To reconcile these differences and ensure that the proposed AADC is as effective as possible, we made several policy recommendations calling for more precise implementation guidelines, better enforcement mechanisms, greater transparency of industry practices on children’s data, and leveraging preliminary data from the U.K. to help alleviate industry fears around these new regulations within the U.S.

## Appendix:

### A1. Copy of Interval Review Board (IRB) Application (Entire Team)

<https://drive.google.com/file/d/1S5MzPPFRd4gLX5XzYo6m0sPoPNCBCR8n/view?usp=sharing>

### A2. CSV Files of Website Annotations (Morgan, Varun)

[https://docs.google.com/spreadsheets/d/1-pzX24q45rcA31y9bGS\\_QjuBhJiT6kKDggqXPyZB5G4/edit#gid=1572347475](https://docs.google.com/spreadsheets/d/1-pzX24q45rcA31y9bGS_QjuBhJiT6kKDggqXPyZB5G4/edit#gid=1572347475)

### A3. Screenshot of Interview Contact Log (Cybèle)



Date First Contacted	Follow-up Date	Method	Name	Title	Company	Response?	Interview Date
<b>Industry Representatives:</b>							
12/11/2022	N/A	Email	Spyro Karetos	Chief Compliance Officer	Google	12/12/2022	DECLINED
12/11/2022	12/19/2022	LinkedIn	Michael Mangold	Head of Risk and Compliance	YouTube	None	
12/11/2022	N/A	LinkedIn	Randall Ortman	Privacy Counsel	Google	None	
12/11/2022	12/19/2022	LinkedIn	Erica Finkle	Director, Policy	Meta	None	
12/11/2022	12/19/2022	LinkedIn	Megan McLarmon	Privacy & Data Policy, Youth Lead	Meta	None	
12/11/2022	12/19/2022	LinkedIn	Juliana Cotto	Privacy Policy Manager, Youth	Meta	None	
12/11/2022		LinkedIn	Jasmine Park	Policy Strategist for Kids & Family	Google	None	
12/11/2022		LinkedIn	Jeb Head	Policy Enforcement Manager	YouTube	None	
12/11/2022		LinkedIn	Pia Shah	Global Head of Policy, Trust & Safety	Amazon	None	
12/11/2022		LinkedIn	Letitia Wong	Director, Data Privacy Policy	Yahoo	None	
12/11/2022		LinkedIn	Aki Nakanishi	Lead Privacy Program Manager	Wikipedia	None	
12/11/2022		LinkedIn	Vaishnavi J.	Head of Youth Wellbeing	Meta	None	
12/11/2022	12/19/2022	LinkedIn	Ivan Rosario	Associate Principal Counsel	ESPN	None	
12/11/2022		LinkedIn	Benjamin Lee	VP and General Counsel	Reddit	None	
12/11/2022		LinkedIn	Thomas Lee	Director, Associate General Counsel	Reddit	12/11/2022	DECLINED
12/11/2022		LinkedIn	Sara Lynch	Privacy Counsel	LinkedIn	None	
12/11/2022		LinkedIn	Lara Hoffman	VP, Privacy & Security	Netflix	None	
12/11/2022		Email	Tanya Forsheit	Head of Privacy Compliance	NYTimes	12/13/2022	DECLINED
12/11/2022		LinkedIn	Liz Roberts	Senior Privacy Counsel	DuckDuckGo	None	
12/11/2022		LinkedIn	Krystyl Mainenschein	Privacy Manager	Walmart	None	
12/11/2022		LinkedIn	Angela Sherrer	VP & Chief Counsel, Data & Technology	Walmart	None	
12/11/2022		LinkedIn	Nuala O'Connor	SVP & Chief Counsel, Digital Citizenship	Walmart	12/11/2022	DECLINED
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Patrick Dillon-Hughes	Global Head of Privacy	Pinterest	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Claire Gartland	Global Product Policy Lead, Youth Safety & W	TikTok	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Catherine Razzano	Head of Global Legal Compliance	TikTok	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Jessica Ashooh	Senior Director of Policy	Reddit	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Desmond Cussen	General Counsel	Fandom	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Stacy Carmody	Corporate Counsel, Privacy	Indeed	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Matthew J.	Data Privacy & Security Attorney (DPO)	Indeed	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Steve Bené	General Counsel	Twitch	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Michael Hill	Privacy & Data Governance	Twitch	None	
12/11/2022		LinkedIn Sales Navigator	Amber Mednick	Senior Corporate Counsel, Privacy	T-Mobile	None	
12/11/2022		LinkedIn Sales Navigator	Kelsey Joyce	Chief Privacy Officer & VP	T-Mobile	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Courtney Bowman	Associate Principal Counsel, Privacy	Hulu (Disney)	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Cindy McEvoy	Assistant General Counsel	Hulu (Disney)	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Cathie Tong	Associate Principal Counsel	Hulu (Disney)	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Janine Castornia	Chief Privacy Officer	USPS	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Michele Muleady	Chief Privacy Officer	USPS	None	
12/11/2022		LinkedIn Sales Navigator	Jason Yurasek	General Counsel	Craigslist	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Shikha Kamboj	Global Head of Privacy	PayPal	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Stacey Keegan	Chief Privacy Officer & Associate General Co	Home Depot	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	Hailun Ying	Senior Lead Counsel, Privacy	Roblox	None	
12/11/2022	12/19/2022	LinkedIn Sales Navigator	James Webb	Privacy Counsel	Snap Inc	None	
12/12/2022	12/19/2022	LinkedIn Sales Navigator	Louise Diaz	Chief Privacy Officer, Global Privacy Compliar	Amazon	None	
12/12/2022		LinkedIn Sales Navigator	Ashlen Cherry	Senior Manager, Ad Privacy	Amazon	None	
12/12/2022	12/19/2022	LinkedIn Sales Navigator	Senthil Jayavelu	Head of Alexa Privacy Assurance	Amazon	None	
12/12/2022		LinkedIn Sales Navigator	Phillip Jackman	Principal Counsel	Disney	None	
12/12/2022		LinkedIn Sales Navigator	Lisa Phua	Principal Counsel	Disney	None	
12/12/2022		LinkedIn Sales Navigator	Alysha Rajnarine	Principal Counsel	National Geographic	None	
12/12/2022		LinkedIn Sales Navigator	Peter Jaffe	VP & Senior Associate General Counsel	National Geographic	None	
12/12/2022		LinkedIn Sales Navigator	Sara DeWitt	SVP & GM	PBS Kids	None	
12/12/2022		LinkedIn Sales Navigator	Walter Stillwell	VP, Legal	PBS Kids	None	
12/12/2022		Email	Adam Lentz	Legal lead on COPPA	Walmart	12/12/2022	12/19/2022
<b>UK ICO Representatives:</b>							
12/11/2022	N/A	Email	Michael Murray	Head of Department: Regulatory Strategy Sen	UK ICO	12/12/2022	12/20/2022
12/11/2022	N/A	Email	Julia Cooke	Principal Policy Adviser	UK ICO	12/12/2022	12/20/2022
12/11/2022	N/A	LinkedIn	Ahmed Razek	Principal Technology Advisor - AI	UK ICO (former)	12/11/2022	12/15/2022