September 30, 2020

Joseph A. Cannataci

Special Rapporteur on the Right to Privacy
Office of the United Nations High Commissioner for Human Rights
Palais Wilson

52 rue des Pâquis

CH-1201 Geneva, Switzerland

**RE: ACT | The App Association Comments Regarding the Special Rapporteur’s Upcoming Report to the Human Rights Council, ‘A Better Understanding of Privacy: Children’s right to Privacy’**

1. **Statement of Interest & General Comments on Children’s Privacy**

ACT | The App Association (App Association) appreciates the opportunity to provide input regarding the privacy rights of children (noted by the Special Rapporteur’s request for input as being under the age of 18) and issues relating to their independence and autonomy.[[1]](#footnote-1) Of the areas of interest raised by the Special Rapporteur, these comments will primarily focus on “the strengths and challenges of ‘age based’ and ‘age verification’ approaches”, as well as “governmental or other structures including regulatory arrangements, established to advance the human rights of the child”.

1. **Introduction and Statement of Interest**

The App Association represents approximately 5,000 small business software application development companies and technology firms globally that create the technologies driving internet of things (IoT) use cases across consumer and enterprise contexts. Today, the App Association represents an ecosystem valued at approximately $1.7 trillion USD globally. Our members create innovative solutions that drive the world’s rapid embrace of mobile technology. Their products power consumer and enterprise markets across modalities and segments of the global economy.

The App Association takes an active role to ensure that the small business community is aware of their responsibilities under applicable children’s laws and regulations. In the United States, those efforts are most commonly directed toward the Children’s Online Privacy Protection Act (COPPA) Rule, implemented, overseen, and enforced by the Federal Trade Commission (FTC). For example, the App Association created a checklist for apps that are made for children to ensure that there is a free accessible resource for small businesses to use as a guide to comply with the COPPA Rule.[[2]](#footnote-2) In addition, our organization consistently participates in public forums on the issue of protecting children with respect to technology and mobile apps. We testified before the House Energy and Commerce Committee on “Protecting Children’s Privacy in an Electronic World”[[3]](#footnote-3); participated in the FTC’s “The Future of the COPPA Rule” workshop[[4]](#footnote-4); and most recently spoke at the Family Online Safety Institute’s (FOSI) 2019 Annual Conference.[[5]](#footnote-5)

App Association members take the privacy and security of children very seriously and seek to exceed legal requirements due to a commitment to a safe experience for children (and their parents) online and through apps. In our experience, children’s privacy laws and regulations that take overly prescriptive approaches, especially relative to obtaining parental consent, actually disincentivize good-faith compliance, driving providers to less regulated corners of the internet and reducing the market for children-directed apps and services. The net effect is a less protective and competitive children’s product marketplace. We strongly urge governments to ensure that laws and regulations do not discourage or cast out any new innovations that may enable improved and streamlined information society services while protecting children’s privacy. We urge the United Nations (UN) and governments to take a "do no harm" approach to new and innovative services in its efforts to protect children’s privacy.

Governments are also strongly encouraged to base laws and regulations protecting children’s privacy on demonstrated harms and verifiable data. For example, the App Association has encountered government proposals to prohibit mechanisms such as reward loops, continuous scrolling, notifications, and auto-play features despite an undocumented relationship to children’s health and wellbeing. The App Association opposes such prohibitions without a firm evidence base first being established. Governments should base laws and regulations on comprehensive evidence-based analyses, and not fringe or hypothetical use cases.

We encourage governments to ease compliance burdens by detailing numerous use cases showing what that government believes is appropriate as well as inappropriate under the applicable regulation. Such an approach will make the laws and regulations much more actionable to stakeholders, particularly small business innovators who do not have extensive budgets for compliance projects.

1. **Current State of Children’s Online Usage and Parent Engagement Impacting Businesses’ Operations Under Laws and Regulations Addressing Children’s Privacy**

App Association members work hard to clearly communicate settings, tiers, etc., to users that can be relied upon. According to the App Association’s research, 85 percent of parents have concerns about their children’s digital privacy.[[6]](#footnote-6) PricewaterhouseCoopers (PwC) says that kids 12 to 15 years old consume 20 hours of screen time each week,[[7]](#footnote-7) with other data suggesting that kids eight to 18 years old consume seven hours of screen time per day.[[8]](#footnote-8) This increased amount of screen time in children eight to 18, in combination with the high percentage of parental concern, one would assume that parents would actively take steps to address their children’s screen time. These steps include enabling parental control settings on their children’s’ devices to make sure they do not have access to inappropriate information and reading privacy policies that the child may not understand due to their age and lack of life experience. Further research shows that fewer than one in three parents use parental settings on their children’s device,[[9]](#footnote-9) while the Pew Research Center also says that 81 percent of parents knowingly let their children use General Audience (GA) YouTube without parental restrictions.[[10]](#footnote-10)

These research results from a variety of sources demonstrate that while parents often say they care deeply about their children’s privacy, their actions display a lesser degree of concern. They may also feel that they should not be the ones responsible for setting the parental controls in place. Instead parents would prefer that app developers provide free educational applications that help their child learn how to read, understand their multiplication tables, or provide some entertainment with the needed privacy provisions already in place to protect their children. However, developers with children-directed apps must balance using financial resources to stand out in a competitive app market with the costs of complying with general privacy laws as well as children’s privacy laws and regulations. This balance leads to many developers deciding to exclusively develop products for a general audience as opposed to for a child’s use. Furthermore, others position their products to avoid being subject to children’s privacy laws and regulations and instead sell their products to schools (where they may be subject to separate requirements as a result).

Implementation of the COPPA Rule in the United States illustrates the danger of overly prescriptive regulatory structures. Because regulator-approved methods for obtaining verifiable parental consent (VPC) under the rule (which include faxing consent forms to the app provider or service or dialing into a dedicated call center) are so outdated and arduous, many creators of children’s-oriented websites and services have either abandoned the sector or tinkered with their marketing to appear as a general audience product ostensibly patronized by non-child users and thus not subject to COPPA. The latter practice is fairly widespread and often brazen; companies such as YouTube[[11]](#footnote-11) and TikTok[[12]](#footnote-12), which profit from popular accounts held and watched by users clearly under the age of 13, claimed general audience status, flouting COPPA and the FTC by ignoring their responsibility to obtain VPC. Though the FTC recently reached settlements with both companies, the fines they are required to pay pale in comparison from the benefits they accrued from ignoring the law.[[13]](#footnote-13)

It is imperative that governments find a new and balanced approach between the importance of children’s privacy and a reasonable cost of compliance. For example, governments should address where liability begins and ends in the context of third parties (e.g., platforms, plug-in creators, and analytics providers). Such third parties may have no idea as to whether the innovation they provide is being used in a way that would give rise to compliance obligations under children’s privacy rules. The App Association requests that, when a third party is not clearly informed that the product or service it is providing is intended to be used by children, it shall not face liability under the laws and regulations protecting children’s privacy. Without this important clarification, it would force such third parties to take severe steps to prevent liability exposure, unfairly raising the costs of development for small business software service providers.

1. **Strengths and Challenges of ‘Age Based’ and ‘Age Verification’ Approaches**

The App Association believes that robust age verification will provide the clearest evidence of what ages are intended to use a service. Several practical children’s privacy- related compliance challenges arise from the fact that many apps integrate into and operate through mobile communications platforms maintained by a different operator. As a result, certain information—such as the user's IP address, device ID, username, or screen name—sometimes shares automatically between the app developer and the platform provider when a user runs the application. This limited information sharing supports (and is often necessary for) the technical and operational functioning of the app.

To the extent that regulatory structures apply ‘aged-based’ or ‘age verification’ approaches to obtaining parental consent, the App Association urges governments to permit more efficient and practical solutions for compliance that take advantage of the latest pro-consumer developments in technology. We see parental consent as three separate and distinct steps:

1. Verifying that the person who will be providing consent is an adult.
2. Notifying the consenting adult of the intended collection, use, and disclosure of the child's personal information by the app developer, consistent with the disclosures made in the privacy notice.
3. Obtaining consent from the adult of behalf of a child that the app is permitted to collect, use, or disclose personal information provided in the notice.

The App Association encourages governments to allow platforms to innovate around tools and mechanisms for app developers to utilize as they implement the three steps to obtain parental consent. A potential innovation could include a mechanism to verify that a person is an adult and able to consent to an app’s privacy policy of behalf of a child, or the first step of parental consent. Additionally, the platform can provide the consenting adult with a notification of the collection, use, or disclosure of the child’s personal information in accordance with the second step of parental consent. Finally, a platform may provide implementation methods to the app developer around ways in which the app developer may obtain verifiable parental consent from the parent. However, it is the sole responsibility of the app developer to select and obtain compliant parental consent from the parent for the collection, use, or disclosure of the child’s personal information. As a result of these collaborative efforts by platforms and app developers, parents can make informed decisions about the apps their children use in an exponentially streamlined and transparent fashion.

The App Association notes that some platforms already implement similar procedures by offering family plans to sign up and use a platform along with providing parents optional settings for their children such as ‘asking to buy,’ rejecting or approving a purchase, monitoring content, or placing limits on screen time from the parent’s device.[[14]](#footnote-14) This allows a parent a simplified process to see what their kids are doing on their devices and decide what limits they want to set for their children, ensuring that parents have meaningful notice of and control over how an app collects, uses, and discloses their children's personal information without imposing unnecessary burdens and costs on app developers.

1. **Personal Information Should Not Include a Child’s Unidentifiable Biomarkers**

Across modalities, children are accessing (and contributing) online content at younger and younger ages. Many households use Apple’s Siri ®, Amazon’s Alexa ®, and Google’s Google HomeTM, and it is inevitable that the device or an application on the device may pick up a child’s voice, often without it knowing due to its inability to detect the difference. Another common device used in the home by kids is a video game console, such as Microsoft’s Xbox and Sony’s PlayStation 4®, which allows the child to talk to other users online. Furthermore, there are applications made for individuals with learning or physical disabilities to help them in their everyday lives and enable them to have independence from a caretaker. For example, autistic children could be using an app to help them with their speech, which would require the collection of the child’s voice in order to make their statement clearer; or a child who is blind may also speak to the virtual assistant software in their phone in order to use the phone’s basic functions.

Many new apps may collect biomarkers such as voice, facial features, and fingerprints in some form, and the App Association urges governments to consider how these latest technologies can adhere to and advance the purpose of (often outdated) laws and regulations addressing children’s privacy. We urge governments to recognize the extraordinary burdens associated with children’s privacy laws and regulations compliance, particularly for small business developers of such technology. For example, developing additional technology to identify the difference between an adult and child voice remains a need, and its implementation may be prohibitively expensive while providing no additional protections for the child if the biomarker is deidentified. The App Association fully supports privacy protections for children, but we all lose if we continue to disincentivize the development of such tech through potentially unfeasible regulatory requirements.

Therefore, the App Association strongly urges governments to ensure that their definition of personal information either excludes ‘biomarkers’ or to only require that a business comply with children’s privacy laws and regulations when identifying, or reasonably identifying, the ‘biomarker’ and specifically associating it with the child as opposed to the child’s voice only being generally wrapped up in a data collection by an app.

1. **Conclusion**

The App Association’s members work hard to positively change children’s lives through smart device applications that help them learn, explore, and communicate. Our members include countless parents who are developers, and they understand the need to protect children in the mobile and internet environment. There is no stronger group of people with the knowledge and the frontline experience to understand that privacy and innovation can coexist. What can create conflict is well-meaning regulation that errs on the side of proscribing innovation in the name of protecting privacy.

We thank the Special Rapporteur in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,



Brian Scarpelli

Senior Global Policy Counsel

Matt Schwartz

ACT | The App Association

1401 K St NW (Ste 501)

Washington, DC 20005

e: bscarpelli@actonline.org

1. <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_July_SRP_Call_for_Submissions_and_Note.pdf>. [↑](#footnote-ref-1)
2. <https://actonline.org/family-app-privacy/> [↑](#footnote-ref-2)
3. U.S. House Energy & Commerce Committee, Hearing, Protecting Children's Privacy in an Electronic World (Oct. 5, 2011). [↑](#footnote-ref-3)
4. The Federal Trade Commission, *The Future of COPPA Rule Workshop*: Morgan Reed, President, ACT | The App Association, *Developers and COPPA: Their Real-World Experience*, (Oct. 7, 2019), <https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop>. [↑](#footnote-ref-4)
5. Family Online Safety institute (FOSI), *2020 Vision: The Future of Online Safety*, (November 21, 2019) <https://www.fosi.org/events/2019-annual-conference/>. [↑](#footnote-ref-5)
6. Morgan Reed, *Developers and COPPA: Their Real-World Experience*, F.T.C. COPPA Workshop, <https://www.ftc.gov/system/files/documents/public_events/1535372/slides-coppa-workshop-10-7-19.pdf> (October 7, 2019) (F.T.C. COPPA Workshop Slides). [↑](#footnote-ref-6)
7. *Kids Digital Media Report 2019*, PriceWaterhouseCoopers, 4, [https://cdn2.hubspot.net/hubfs/5009836/PwC%202019/Kids%20Digital%20Media%20Report%202019%20.pdf?](https://cdn2.hubspot.net/hubfs/5009836/PwC%202019/Kids%20Digital%20Media%20Report%202019%20.pdf) (May 2019). [↑](#footnote-ref-7)
8. *New tools, old rules: limit screen-based recreational media at home*, American Heart Association Scientific Advisory, <https://newsroom.heart.org/news/new-tools-old-rules-limit-screen-based-recreational-media-at-home> (Aug. 6, 2018). [↑](#footnote-ref-8)
9. F.T.C. COPPA Workshop Slides. [↑](#footnote-ref-9)
10. Aaron Smith, et. al, *Many Turn to YouTube for Children’s Content, News, How-To Lessons*, Pew Research Center, <https://www.pewresearch.org/internet/2018/11/07/many-turn-to-youtube-for-childrens-content-news-how-to-lessons/> (Nov. 7, 2018). [↑](#footnote-ref-10)
11. Federal Trade Commission. “Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children’s Privacy Law” (September 4, 2019).

<https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> [↑](#footnote-ref-11)
12. Federal Trade Commission. “Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children’s Privacy Law” (February 27, 2019).

<https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc> [↑](#footnote-ref-12)
13. Federal Trade Commission. “Dissenting Statement of Commissioner Rohit Chopra in the Matter of Google, LLC and YouTube, LLC” (September 4, 2019).

<https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf> [↑](#footnote-ref-13)
14. *Keep Your Child’s Screen Time Healthy and Happy*, Qustodio, [qustodio.com/en/family/how-it-works/](http://qustodio.com/en/family/how-it-works/) (last visited December 11, 2019) (explaining how Qustodio’s program helps parents manage and supervise their children’s devices); *Family Privacy Disclosure for Children*, Apple, <https://www.apple.com/legal/privacy/en-ww/parent-disclosure/> (last visited December 11, 2019). [↑](#footnote-ref-14)